EXHIBIT C

PLR 4-3(b) – Identification of Supporting Evidence

The following represents InterTrust's list of evidence relevant to construction of the disputed terms and phrases.

Notes:

1. InterTrust reserves the right to supplement this list as needed to respond to changed constructions proffered by Microsoft. InterTrust also reserves the right to rely on evidence cited in the original version of this Exhibit, filed February 3, 2003.

2. In the following list, certain terms and phrases include other, separately defined terms. In such cases, the evidence supporting the separately defined term is also relevant to construction of the larger term.

3. The InterTrust patents include overlapping specifications, in which the same text may be found in two or more specifications. Where only one of the specifications is cited, InterTrust reserves the right to substitute citations for the same text in the other specifications.

4. Highlighting has been used to indicate added emphasis.

5. Each claim term is followed by a list of all patent claims in which the term appears (e.g., "193.15" means claim 15 from the '193 patent).

Key to abbreviations:
USP = United States Patent
'193 patent = USP 6,253,193
'683 patent = USP 6,185,683
'721 patent = USP 6,157,721
'891 patent = USP 5,982,891
'861 patent = USP 5,920,861
'912 patent = USP 5,917,912
'900 patent = USP 5,892,900

	Claim Term / Phrase	InterTrust Evidence
1.	**aspect** 683.2, 861.58, 900.155, 912.8	**Patent Specifications** **1(A)** This reinitialization mechanism would permit CPU/SPU 2650 to be initialized several times, facilitating testing and/or re-use for different applications, while protecting all security-relevant aspects of its operation. '900 patent at 77:15-19. **1(B)** In addition, the overall software-based tamper resistant barrier 674 and associated PPE system is sufficiently complex so that it is difficult to tamper with a part of it without destroying other aspects of its functionality (i.e., a "defense in depth"). '900 patent at 236:3-7. **1(C)** As with any system incorporating "applications" and "operating systems," the boundary between these aspects of an overall system can be ambiguous. '193 patent at 83:30-32. **1(D)** Since SPE 503 in the preferred embodiment runs within the confines of an SPU 500, one aspect of this device driver 736 is to provide low level communications services with the SPU 500 hardware. '193 patent at 95:27-30. **1(E)** Templates may present one or more models that describe various

	Claim Term / Phrase	InterTrust Evidence
		aspects of a content object and how the object should be created including employing secure atomic methods that are used to create, alter, and/or destroy permissions records 808 and/or associated budgets, etc. '193 patent at 260:42-47. **1(F)** In accordance with one aspect of how to advantageously use descriptive data structures in accordance with a preferred embodiment of this invention, a machine readable descriptive data structure may be created by a provider to describe the layout of the provider's particular rights management data structure(s) such as secure containers. '861 patent at 6:24-29. **1(G)** Controls 316 may provide rules and associated consequences for controlling or otherwise affecting the use or other aspects of what value chain participant 602 can do with DDS 200. '861 patent at 17:3-6.

	Claim Term / Phrase	InterTrust Evidence
2.	**authentication** 193.15	**Patent Specifications** **2(A)** To increase the security of security barrier 502 even further, it is possible to encase or include SPU 500 in one or more further physical enclosures such as, for example: epoxy or other "potting compound"; further module enclosures including additional self-destruct, self-disabling or other features activated when tampering is detected; further modules providing additional security protections such as requiring password or other authentication to operate; and the like. '193 patent at 64:29-37. **2(B)** It may also or alternatively provide or include one or more passwords or other information used to identify or otherwise verify/authenticate an individual's identity, such as voice print and retinal scan information. '193 patent at 236:21-25. **2(C)** This certification process in the preferred embodiment may be used to permit a VDE electronic appliance to present one or more "certificates" authenticating that it (or its key) can be trusted. As described above, this "certification" process may be used by one PPE 650 to "certify" that it is an authentic VDE PPE, it has a certain level of security and capability set (e.g., it is hardware based rather than merely software based), etc. Briefly, the "certification" process may involve using a certificate private key of a certification key pair to encrypt a message including another VDE node's public-key. The private key of a certification key pair is preferably used to generate a PPE certificate. It is used to encrypt a public-key of the PPE. A PPE certificate can either be stored in the PPE, or it may be stored in a certification repository. '193 patent at 213:1-15.

	Claim Term / Phrase	InterTrust Evidence
		2(D) SPE Authentication Manager/Service Communications Manager 564 The Authentication Manager/Service Communications Manager 564 supports calls for user password validation and "ticket" generation and validation. It may also support secure communications between SPE 503 and an external node or device (e.g., a VDE administrator or distributor). It may support the following examples of authentication-related service requests in the preferred embodiment: Call Name — Description User Services Create User — Creates a new user and stores Name Services Records (NSRs) for use by the Name Services Manager 752. Authenticate User — Authenticates a user for use of the system. This request lets the caller authenticate as a specific user ID. Group membership is also authenticated by this request. The authentication returns a "ticket" for the user. '193 patent at 123:21-42.

	Claim Term / Phrase	InterTrust Evidence
3.	budget 193.1	**Patent Specifications** **3(A)** PERC 808 may also contain or refer to budgets containing potentially valuable quantities/values. Such budgets may be stored within a traveling object itself, or they may be delivered separately and protected by highly secure communications keys and administrative object keys and management database techniques. '193 patent at 132:60-65. --- **3(B)** User Data Elements (UDEs) 1200 and Method Data Elements (MDEs) 1202 in the preferred embodiment store data. There are many types of UDEs 1200 and MDEs 1202 provided by the preferred embodiment. In the preferred embodiment, each of these different types of data structures shares a common overall format including a common header definition and naming scheme. Other UDEs 1200 that share this common structure include "local name services records" (to be explained shortly) and account information for connecting to other VDE participants. These elements are not necessarily associated with an individual user, and may therefore be considered MDEs 1202. All UDEs 1200 and all MDEs 1202 provided by the preferred embodiment may, if desired, (as shown in Figure 16) be stored in a common physical table within secure database 610, and database access processes may commonly be used to access all of these different types of data structures. In the preferred embodiment, PERCs 808 and user rights table records are types of UDE 1200. There are many other types of UDEs 1200/MDEs 1202, including for example, meters, meter trails, budgets, budget trails, and audit trails. '193 patent at 142:41-61. --- **3(C)** In the example shown in Figure 41d, a distributor at a VDE distributor node (106) might request budget from a content creator at another node (102). This request may be made in the context of a secure VDE communication or it may be passed in an "out-of-

	Claim Term / Phrase	InterTrust Evidence
		channel" communication (e.g. a telephone call or letter). The creator 102 may decide to grant budget to the distributor 106 and processes a distribute event (1452 in BUDGET method 1510 at VDE node 102). A result of processing the distribute event within the BUDGET method might be a secure communication (1454) between VDE nodes 102 and 106 by which a budget granting use and redistribute rights to the distributor 106 may be transferred from the creator 102 to the distributor. The distributor's VDE node 106 may respond to the receipt of the budget information by processing the communication using the reply process 1475B of the BUDGET method 1510. The reply event processing 1475B might, for example, install a budget and PERC 808 within the distributor's VDE 106 node to permit the distributor to access content or processes for which access is control at least in part by the budget and/or PERC. At some point, the distributor 106 may also desire to use the content to which she has been granted rights to access. After registering to use the content object, the user 112 would be required to utilize an array of "use" processes 1476C to, for example, open, read, write, and/or close the content object as part of the use process. Once the distributor 106 has used some or all of her budget, she may desire to obtain additional budget. The distributor 106 might then initiate a process using the BUDGET method request process (1480B). Request process 1480B might initiate a communication (1482AB) with the content creator VDE node 102 requesting more budget and perhaps providing details of the use activity to date (e.g., audit trails). The content creator 102 processes the 'get more budget request event 1482AB using the response process (1484A) within the creator's BUDGET method 1510A. Response process 1484A might, for example, make a determination if the use information indicates proper use of the content, and/or if the distributor is credit worthy for more budget. The BUDGET method response process 1484A might also initiate a financial transaction to transfer funds from the distributor to pay for said use, or use the distribute process 1472A to distribute budget to the distributor 106. A response to the distributor 106 granting more budget (or denying more budget) might be sent immediately as a response to the request communication 1482AB, or it might be sent at a later time as part of a separate communication. The response communication, upon being received at the distributor's VDE node 106, might be processed using the reply process 1475B within the distributor's copy of the BUDGET method 1510B. The reply process 1475B might then process the additional budget in the same manner as described above.

	Claim Term / Phrase	InterTrust Evidence
		The chain of handling and control may, in addition to posting budget information, also pass control information that governs the manner in which said budget may be utilized. For example, the control information specified in the above example may also contain control information describing the process and limits that apply to the distributor's redistribution of the right to use the creator's content object. Thus, when the distributor responds to a budget request from a user (a communication between a user at VDE node 112 to the distributor at VDE node 106 similar in nature to the one described above between VDE nodes 106 and 102) using the distribute process 1472B within the distributor's copy of the BUDGET method 1510B, a distribution and request/response/reply process similar to the one described above might be initiated. '193 patent at 172:61-174:29. **3(D)** BILLING method 406 may then pass the event on to a BUDGET method 408. BUDGET method 408 sets limits and records transactional information associated with those limits. For example, BUDGET method 408 may store budget information in a budget UDE, and may store an audit record in a budget trail UDE. BUDGET method 408 may result in a "budget remaining" field in a budget UDE being decremented by an amount specified by BILLING method 406. '193 patent at 182:22-30. **3(E)** BUDGET method 1510 may read and update budget information within a BUDGET method UDE, '193 patent at 184:67-185:1. **3(F)** Figure 5A shows how the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a "container" 302 so the information can't be accessed except as

	Claim Term / Phrase	InterTrust Evidence
		provided by its "rules and controls." Normally, the container 302 is electronic rather than physical. Electronic container 302 in one example comprises "digital" information having a well defined structure. Container 302 and its contents can be called an "object 300." The Figure 5A example shows items "within" and enclosed by container 302. However, container 302 may "contain" items without those items actually being stored within the container. For example, the container 302 may reference items that are available elsewhere such as in other containers at remote sites. Container 302 may reference items available at different times or only during limited times. Some items may be too large to store within container 302. Items may, for example, be delivered to the user in the form of a "live feed" of video at a certain time. Even then, the container 302 "contains" the live feed (by reference) in this example. Container 302 may contain information content 304 in electronic (such as "digital") form. Information content 304 could be the text of a novel, a picture, sound such as a musical performance or a reading, a movie or other video, computer software, or just about any other kind of electronic information you can think of. Other types of "objects" 300 (such as "administrative objects") may contain "administrative" or other information instead of or in addition to information content 304. In the Figure 5A example, container 302 may also contain "rules and controls" in the form of: (a) a "permissions record" 808; (b) "budgets" 308; and (c) "other methods" 1000. Figure 5B gives some additional detail about permissions record 808, budgets 308 and other methods 1000. The "permissions record" 808 specifies the rights associated with the object 300 such as, for example, who can open the container 302, who can use the object's contents, who can distribute the object, and what other control mechanisms must be active. For example, permissions record 808 may specify a user's rights to use, distribute and/or administer the container 302 and its content. Permissions record 808 may also specify requirements to be applied by the budgets 308 and "other methods" 1000. Permissions record 808 may also contain security related information such as scrambling and descrambling "keys."

	Claim Term / Phrase	InterTrust Evidence
		"Budgets" 308 shown in Figure 5B are a special type of "method" 1000 that may specify, among other things, limitations on usage of information content 304, and how usage will be paid for. Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget. "Other methods" 1000 define basic operations used by "rules and controls." Such "methods" 1000 may include, for example, how usage is to be "metered," if and how content 304 and other information is to be scrambled and descrambled, and other processes associated with handling and controlling information content 304. For example, methods 1000 may record the identity of anyone who opens the electronic container 302, and can also control how information content is to be charged based on "metering." Methods 1000 may apply to one or several different information contents 304 and associated containers 302, as well as to all or specific portions of information content 304. '193 patent at 58:38-59:37. **3(G)** FIGURES 5A and 5B show an example of an "object"; '193 patent at 50:18. **3(H)** Field type / Format / Typical Use / Description or Use Ascending Use Counter — byte, short, long, or unsigned versions of the same widths — Meter/ Budget — Ascending count of uses. Descending Use Counter — byte, short, long, or unsigned — Budget — Descending count of permitted use; e.g., remaining

	Claim Term / Phrase	InterTrust Evidence
		versions of the same widths budget '193 patent at 143:57-65.
		3(I) As with standard VDE objects 300, a user may be required to contact a clearinghouse service to acquire additional budgets if the user wishes to continue to use the traveling object after the exhaustion of an available budget(s) . . . . '193 patent at 131:10-13.
		3(J) Once the distributor 106 has used some or all of her budget, she may desire to obtain additional budget. The distributor 106 might then initiate a process using the BUDGET method request process (1480B). Request process 1480B might initiate a communication (1482AB) with the content creator VDE node 102 requesting more budget and perhaps providing details of the use activity to date (e.g., audit trails). The content creator 102 processes the 'get more budget' request event 1482AB using the response process (1484A) within the creator's BUDGET method 1510A. Response process 1484A might, for example, make a determination if the use information indicates proper use of the content, and/or if the distributor is credit worthy for more budget. The BUDGET method response process 1484A might also initiate a financial transaction to transfer funds from the distributor to pay for said use, or use the distribute process 1472A to distribute budget to the distributor 106. A response to the distributor 106 granting more budget (or denying more budget) might be sent immediately as a response to the request communication 1482AB, or it might be sent at a later time as part of a separate communication. The response communication, upon being received at the distributor's VDE node 106, might be processed using the reply process 1475B within the distributor's copy of the BUDGET method 1510B. The reply process 1475B might then process the additional budget in the same manner as described above. '193 patent at 173:21-174:14.

	Claim Term / Phrase	InterTrust Evidence
		3(K) During the same or different communications exchange, the same or different clearinghouse may handle the end user's request for additional budget and/or permission pertaining to VDE object 300. For example, the end user's electronic appliance 600 may (e.g., in response to a user input request to access a particular VDE object 300) send an administrative object to the clearinghouse requesting budgets and/or other permissions allowing access (Block 1164). As mentioned above, such requests may be transmitted in the form of one or more administrative objects, such as, for example, a single administrative object having multiple "events" associated with multiple requested budgets and/or other permissions for the same or different VDE objects 300. The clearinghouse may upon receipt of such a request, check the end user's credit, financial records, business agreements and/or audit histories to determine whether the requested budgets and/or permissions should be given. The clearinghouse may, based on this analysis, send one or more responsive administrative objects which cause the end user's electronic appliance 600 to update its secure database in response (Block 1166, 1168). This updating might, for example, comprise replacing an expired PERC 808 with a fresh one, modifying a PERC to provide additional (or lesser) rights, etc. Steps 1164-1168 may be repeated multiple times in the same or different communications session to provide further updates to the end user's secure database 610. '193 patent at 162:39-65. --- **Extrinsic Sources** **3(L)** **budget** *n.* **1.a.** An itemized summary of estimated or intended expenditures for a given period along with proposals for financing them: *submitted the annual budget to Congress.* **b.** A systematic plan for the expenditure of a usually fixed resource, such as money or time, during a given period: *A new car will not be part of our budget this year.* **c.** The total sum of money allocated for a particular purpose or period of time: *a project with an annual budget of five million dollars.* **2.** A stock or collection with definite limits: "*his budget of general knowledge.*" (William Hazlitt). – **budget** *v.* **—et-ed, et-ing, -ets.** *–tr.* **1.** To plan in advance the expenditure of: *needed help budgeting our income; budgeted my time wisely.* **2.** To enter or account for in a budget: *forgot to budget*

	Claim Term / Phrase	InterTrust Evidence
		the car payments. –*intr.* To make or use a budget. –**budget** *adj.* **1.** Of or relating to a budget: *budget items approved by Congress.* **2.** Appropriate to a budget; inexpensive: *a budget car; budget meals.* American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 249.

	Claim Term / Phrase	InterTrust Evidence
4.	clearinghouse 193.19	**Patent Specifications** **4(A)** Clearinghouses may provide independent financial services, such as credit and/or billing services, and can serve as distributors and/or creators. '193 patent at 267:40-42. **4(B)** if appropriate credit (e.g. an electronic clearinghouse account from a clearinghouse such as VISA or AT&T) is available. '193 patent at 25:22-24. **4(C)** clearinghouses that gather usage information regarding, and bill for the use of, electronic information. '193 patent at 3:32-33. **4(D)** in certain models, a clearinghouse might also serve as a rights distribution agent who provides one or more rights to certain value chain participants, which one or more rights may be "attached" to one or more rights to use the clearinghouse's credit (if said clearinghouse is, at least in part, a financial clearinghouse (such a control information provider may alternatively, or in addition, restrict other users' rights. '193 patent at 269:59-65. **4(E)** A document may have an attribute requiring that each use of the document be reported to a central document tracking clearinghouse. This could be used by the organization to track specific documents,

	Claim Term / Phrase	InterTrust Evidence
		to identify documents used by any particular user and/or group of users to track documents with specific attributes (e.g., sensitivity), etc. '193 patent at 280:18-24.
		4(F) In this Figure 2 example, information relating to content use is, as shown by arrow 114, reported to a financial clearinghouse 116. Based on this "reporting," the financial clearinghouse 116 may generate a bill and send it to the content user 112 over a "reports and payments" network 118. Arrow 120 shows the content user 112 providing payments for content usage to the financial clearinghouse 116. Based on the reports and payments it receives, the financial clearinghouse 116 may provide reports and/or payments to the distributor 106. '193 patent at 55:57-66.
		4(G) The "financial clearinghouse" 116 shown in Figure 2 may also be a "VDE administrator." Financial clearinghouse 116 in its VDE administrator role sends "administrative" information to the VDE participants. This administrative information helps to keep the virtual distribution environment 100 operating properly. The "VDE administrator" and financial clearinghouse roles may be performed by different people or companies, and there can be more than one of each. '193 patent at 56:16-24.
		4(H) A summary of the roles of the various participants of virtual distribution environment 100 is set forth in the table below: Role — Description "Traditional" Participants Content creator — Packager and initial distributor of digital

	Claim Term / Phrase	InterTrust Evidence
		information Content Owner — Owner of the digital information. Distributors — Provide rights distribution services for budgets and/or content. Auditor — Provides services for processing and reducing usage based audit trails. Clearinghouse — Provides intermediate store and forward services for content and audit information. Also, typically provides a platform for other services, including third party financial providers and auditors. '193 patent at 255:33-51. **4(I)** Further Chain of Handling Model As described in connection with Figure 2, there are four (4) "participant" instances of VDE 100 in one example of a VDE chain of handling and control used, for example, for content distribution. '193 patent at 253:64-254:1. **4(J)** FIGURE 2 illustrates an example of a chain of handling and control; '193 patent at 50:8-9. **4(K)** a "trusted" financial clearinghouse (e.g., VISA, Mastercard). '193 patent at 41:8-9.

	Claim Term / Phrase	InterTrust Evidence
5.	**compares** 900.155	**Patent Specifications** **5(A)** Comparing Figure 50 with Figure 49 reveals that the same overall high level processing may typically be performed for READ method 1650 as was described in connection with OPEN method 1500. '900 patent at 195:9-12. **5(B)** As compared to Figure 2, Figure 77 includes a new "client administrator" participant 700. '900 patent at 280:63-65. **5(C)** VDE content, and the electronic agreements associated with said content, can be employed and progressively manipulated in commercial ways which reflect traditional business practices for non-electronic products (though VDE supports greater flexibility and efficiency compared with most of such traditional models). '900 patent at 322:15-20. **Extrinsic Sources** **5(D)** **compare** *v. tr.* **1.** To consider or describe as similar, equal, or analogous; liken. **2.** *Abbr.* **cp.** To examine in order to note the similarities or differences of. **3.** *Grammar.* To form the positive, comparative, or superlative degree of (an adjective or adverb). – *intr.* **1.** To be worthy of comparison; bear comparison: *two concert halls that just do not compare.* **2.** To draw comparisons. **comparison** *n.* **1.a.** The act of comparing or the process of being compared. American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 384.

	Claim Term / Phrase	InterTrust Evidence
6.	**component assembly** 912.8, 912.35	**Patent Specifications** **6(A)** ROS VDE functions 604 may be based on segmented, independently loadable executable "component assemblies" 690. These component assemblies 690 are independently securely deliverable. The component assemblies 690 provided by the preferred embodiment comprise code and data elements that are themselves independently deliverable. Thus, each component assembly 690 provided by the preferred embodiment is comprised of independently securely deliverable elements which may be communicated using VDE secure communication techniques, between VDE secure subsystems. These component assemblies 690 are the basic functional unit provided by ROS 602. The component assemblies 690 are executed to perform operating system or application tasks. '193 patent at 83:12-26. **6(B)** Components 690 are preferably designed to be easily separable and individually loadable. ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655). '193 patent at 83:43-48. **6(C)** Thus, the channel 594 is the mechanism in the preferred embodiment that collects together or assembles the elements shown in Figure 11E into a component assembly 690 that may be used for event processing. '193 patent at 115:67-116:4.

	Claim Term / Phrase	InterTrust Evidence
		6(D) In the preferred embodiment, ROS 602 assembles component assemblies 690 based on the following types of elements: Permissions Records ("PERC"s) 808; Method "Cores" 1000; Load Modules 1100; Data Elements (e.g., User Data Elements ("UDEs") 1200 and Method Data Elements ("MDEs") 1202); and Other component assemblies 690. '193 patent at 85:21-29. **6(E)** The selected method event record 1012, in turn, specifies the appropriate information (e.g., load module(s) 1100, data element UDE(s) and MDE(s) 1200, 1202, and/or PERC(s) 808) used to construct a component assembly 690 for execution in response to the event that has occurred. '193 patent at 138:31-36. **6(F)** The reciprocal process 1454 may be based on a component assembly 690 (e.g., one or more load modules 1100, data, and optionally other methods present in the VDE node 600B). '193 patent at 171:39-42. **6(G)** One important security layer involves ensuring that certain component assemblies 690 are formed, loaded and executed only in secure execution space such as provided within an SPU 500. '193 patent at 87:35-38.

	Claim Term / Phrase	InterTrust Evidence
		6(H) ROS 602 provided by the preferred embodiment responds to an event by specifying and beginning processes to process the event. These processes are, in the preferred embodiment, based on methods 1000. Since there are an unlimited number of different types of events, the preferred embodiment supports an unlimited number of different processes to process events. This flexibility is supported by the dynamic creation of component assemblies 690 from independently deliverable modules such as method cores 1000', load modules 1100, and data structures such as UDEs 1200. '193 patent at 169:62-170:4. **6(I)** In the preferred embodiment, ROS 602 assembles securely independently deliverable elements into a component assembly 690 based in part on context parameters (e.g., object, user). '193 patent at 84:17-20. **6(J)** This "channel 0" "open channel" task may then issue a series of requests to secure database manager 566 to obtain the "blueprint" for constructing one or more component assemblies 690 to be associated with channel 594 (block 1127). In the preferred embodiment, this "blueprint" may comprise a PERC 808 and/or URT 464. . . . The preferred embodiment process may next use the "blueprint" to access (e.g, the secure database manager 566 and/or from load module execution manager library(ies) 568) the appropriate "control method" that may be used to, in effect, supervise execution of all of the other methods 1000 within the channel 594 (block 1131). '193 patent at 112:46-51, 112:63-113:2.

	Claim Term / Phrase	InterTrust Evidence
		File Histories **6(K)** Column 1, lines 33-65 [of Fischer 5,748,960] describes "data types" or "classes" in object-oriented programming that meets the term 'component' recited in the instant claims (i.e. code and data elements that are independently deliverable). '912 Patent File History, 9/22/98 Office Action, pp. 2-3.

	Claim Term / Phrase	InterTrust Evidence
7.	**contain** 683.2, 912.8, 912.35	**Patent Specifications** **7(A)** A VDE content container is an object that contains both content (for example, commercially distributed electronic information products such as computer software programs, movies, electronic publications or reference materials, etc.) and certain control information related to the use of the object's content. '193 patent at 19:15-21. --- **7(B)** The Figure 5A example shows items "within" and enclosed by container 302. However, container 302 may "contain" items without those items actually being stored within the container. For example, the container 302 may reference items that are available elsewhere such as in other containers at remote sites. Container 302 may reference items available at different times or only during limited times. Some items may be too large to store within container 302. Items may, for example, be delivered to the user in the form of a "live feed" of video at a certain time. Even then, the container 302 "contains" the live feed (by reference) in this example. '193 patent at 58:48-58. --- **Extrinsic Sources** **7(C)** **contain** *tr.v.* **-tained, -tain-ing, -tains. 1. a.** To have within; hold. **b.** To be capable of holding. **2.** To have as component parts; include or comprise: *The album contains many memorable songs.* **3. a.** To hold or keep within limits; restrain: *I could hardly contain my curiosity.* **b.** To halt the spread or development of; check: *Science sought an effective method of containing the disease.* **4.** To check the expansion or influence of (a hostile power or ideology) by containment. **5.** *Mathematics.* To be exactly divisible by.[Middle English *conteinen*, from Old French *contenir*, from Latin *continere* : *com-*, com- + *tenere*, to hold. See ten-.]**--con-tain'a-ble** *adj.*

	Claim Term / Phrase	InterTrust Evidence
		SYNONYM: *contain, hold, accommodate.* These verbs mean to have within or have the capacity for having within. *Contain* means to have within or have as a part or constituent: *This drawer contains all the cutlery we own. The book contains some amusing passages. Polluted water contains contaminants. Hold* can be used in that sense but primarily stresses capacity for containing: *The pitcher holds two pints but contains only one. Accommodate* refers to capacity for holding comfortably: *The restaurant accommodates 50 customers. Four hundred inmates were crowded into a prison intended to accommodate 200*. American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 406.

	Claim Term / Phrase	InterTrust Evidence
8.	control (n.) 193.1, 193.11, 193.15, 193.19, 891.1	**Patent Specifications** **8(A)** Consumers 206, 208, 210 are each capable of receiving and using the programs created by video production studio 204—assuming, that is, that the video production studio or information utility 200 has arranged for these consumers to have appropriate "rules and controls" (control information) that give the consumers rights to use the programs. '193 patent at 53:53-59. **8(B)** The virtual distribution environment 100 prevents use of protected information except as permitted by the "rules and controls" (control information). For example, the "rules and controls" shown in Figure 2 may grant specific individuals or classes of content users 112 "permission" to use certain content. They may specify what kinds of content usage are permitted, and what kinds are not. They may specify how content usage is to be paid for and how much it costs. As another example, "rules and controls" may require content usage information to be reported back to the distributor 106 and/or content creator 102. '193 patent at 56:26-36. **8(C)** Objects may be classified in one sense based on whether the protection information is bound together with the protected information. For example, a container that is bound by its control(s) to a specific VDE node is called a "stationary object" (see Figure 18). A container that is not bound by its control information to a specific VDE node but rather carries sufficient control and permissions to permit its use, in whole or in part, at any of several sites is called a "Traveling Object".... '193 patent at 129:52-60.

	Claim Term / Phrase	InterTrust Evidence
		8(D) VDEF load modules, associated data, and methods form a body of information that for the purposes of the present invention are called "control information." VDEF control information may be specifically associated with one or more pieces of electronic content and/or it may be employed as a general component of the operating system capabilities of a VDE installation. '193 patent at 18:36-42. **8(E)** Failure information, including the elements listed below, may be saved along with details of the failure: Control Information Retained in an SPE on Access Failures Object ID User ID Type of failure Time of failure This information may be analyzed to detect cracking attempts or to determine patterns of usage outside expected (and budgeted) norms. The audit trail histories in the SPU 500 may be retained until the audit is reported to the appropriate parties. '193 patent at 121:15-32. **8(F)** In this embodiment, the additional memory may be provided by additional one or more integrated circuits that can be contained within a secure enclosure, such as a tamper resistant metal container or some form of a chip pack containing multiple integrated circuit components, and which impedes and/or evidences tampering attempts, and/or disables a portion or all of SPU 500 or associated critical key and/or other control information in the event of tampering. '193 patent at 169:5-13.

	Claim Term / Phrase	InterTrust Evidence
		8(G) . . . may involve preserving at least a portion of the control information (e.g., executable code such as load modules) '193 patent at 33:12-14. **8(H)** VDE control information may, in part or in full, (a) represent control information directly put in place by VDE content control information pathway participants, and/or (b) comprise control information put in place by such a participant on behalf of a party who does not directly handle electronic content (or electronic appliance) permissions records information (for example control information inserted by a participant on behalf of a financial clearinghouse or government agency). Such control information methods (and/or load modules and/or mediating data and/or component assemblies) may also be put in place by either an electronic automated, or a semi-automated and human assisted, control information (control set) negotiating process that assesses whether the use of one or more pieces of submitted control information will be integrated into and/or replace existing control information (and/or chooses between alternative control information based upon interaction with in-place control information) and how such control information may be used. '193 patent at 44:34-52. **8(I)** In either embodiment, certain control information (software and parameter data) must be securely maintained within the SPU, and further control information can be stored externally and securely (e.g. in encrypted and tagged form) and loaded into said hardware SPU when needed. '193 patent at 49:50-55. **8(J)** Content control information governs content usage according to

	Claim Term / Phrase	InterTrust Evidence
		criteria set by holders of rights to an object's contents and/or according to parties who otherwise have rights associated with distributing such content (such as governments, financial credit providers, and users). '193 patent at 15:46-50. **8(K)** VDE's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques. '193 patent at 15:33-38. **8(L)** Control information delivered by, and/or otherwise available for use with, VDE content containers comprise (for commercial content distribution purposes) VDEF control capabilities (and any associated parameter data) for electronic content. These capabilities may constitute one or more "proposed" electronic agreements (and/or agreement functions available for selection and/or use with parameter data) that manage the use and/or the consequences of use of such content and which can enact the terms and conditions of agreements involving multiple parties and their various rights and obligations. '193 patent at 19:22-32. **8(M)** . . . an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). '193 patent at 48:29-34.

	Claim Term / Phrase	InterTrust Evidence
		8(N) In the Figure 5A example, container 302 may also contain "rules and controls" in the form of: (a) a "permissions record" 808; (b) "budgets" 308; and (c) "other methods" 1000. Figure 5B gives some additional detail about permissions record 808, budgets 308 and other methods 1000. The "permissions record" 808 specifies the rights associated with the object 300 such as, for example, who can open the container 302, who can use the object's contents, who can distribute the object, and what other control mechanisms must be active. For example, permissions record 808 may specify a user's rights to use, distribute and/or administer the container 302 and its content. Permissions record 808 may also specify requirements to be applied by the budgets 308 and "other methods" 1000. Permissions record 808 may also contain security related information such as scrambling and descrambling "keys." "Budgets" 308 shown in Figure 5B are a special type of "method" 1000 that may specify, among other things, limitations on usage of information content 304, and how usage will be paid for. Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget. '193 patent at 59:1-25. **8(O)** A distributed database may manage such a distributed repository resource environment and use VDE to secure the storing, communicating, auditing, and/or use of information through VDE's electronic enforcement of VDE controls. '193 patent at 284:22-26. **8(P)** ROS 602 provided by the preferred embodiment extends

	Claim Term / Phrase	InterTrust Evidence
		conventional capabilities such as, for example, Access Control List (ACL) structures, to user and process defined events, including state transitions. ROS 602 may provide full control information over pre-defined and user-defined application events. These control mechanisms include "go/no-go" permissions, and also include optional event-specific executables that permit complete flexibility in the processing and/or controlling of events. This structure permits events to be individually controlled so that, for example, metering and budgeting may be provided using independent executables. For example, ROS 602 extends ACL structures to control arbitrary granularity of information. Traditional operating systems provide static "go-no go" control mechanisms at a file or resource level; ROS 602 extends the control concept in a general way from the largest to the smallest sub-element using a flexible control structure. ROS 602 can, for example, control the printing of a single paragraph out of a document file. '193 patent at 77:45-63. **8(Q)** ROS 602 provided by the preferred embodiment permits secure modification and update of control information governing each component. The control information may be provided in a template format such as method options to an end-user. An end-user may then customize the actual control information used within guidelines provided by a distributor or content creator. '193 patent at 77:64-78:3. **8(R)** VDE control information (e.g., methods) that collectively control use of VDE managed properties (database, document, individual commercial product), are either shipped with the content itself (for example, in a content container) and/or one or more portions of such control information is shipped to distributors and/or other users in separably deliverable "administrative objects." A subset of the methods for a property may in part be delivered with each property while one or more other subsets of methods can be delivered

	Claim Term / Phrase	InterTrust Evidence
		separately to a user or otherwise made available for use (such as being available remotely by telecommunication means). '193 patent at 43:26-37. **8(S)** Many such load modules are inherently configurable, aggregatable, portable, and extensible and singularly, or in combination (along with associated data), run as control methods under the VDE transaction operating environment. '193 patent at 25:48-52. **8(T)** Traveling objects can be used at a receiving VDE node electronic appliance 600 so long as either the appliance carries the correct budget or budget type (e.g. sufficient credit available from a clearinghouse such as a VISA budget) either in general or for specific one or more users or user classes, or so long as the traveling object itself carries with it sufficient budget allowance or an appropriate authorization (e.g., a stipulation that the traveling object may be used on certain one or more installations or installation classes or users or user classes where classes correspond to a specific subset of installations or users who are represented by a predefined class identifiers stored in a secure database 610). After receiving a traveling object, if the user (and/or installation) doesn't have the appropriate budget(s) and/or authorizations, then the user could be informed by the electronic appliance 600 (using information stored in the traveling object) as to which one or more parties the user could contact. '193 patent at 131:33-50. **8(U)** [A]n object provider might allow users to redistribute copies of an object to their friends and associates (for example by physical delivery of storage media or by delivery over a computer network) such that if a friend or associate satisfies any certain criteria required for use of said object, he may do so.

	Claim Term / Phrase	InterTrust Evidence
		For example, if a software program was distributed as a traveling object, a user of the program who wished to supply it or a usable copy of it to a friend would normally be free to do so. Traveling Objects have great potential commercial significance, since useful content could be primarily distributed by users and through bulletin boards, which would require little or no distribution overhead apart from registration with the "original" content provider and/or clearinghouse. The "out of channel" distribution may also allow the provider to receive payment for usage and/or elsewise maintain at least a degree of control over the redistributed object. Such certain criteria might involve, for example, the registered presence at a user's VDE node of an authorized third party financial relationship, such as a credit card, along with sufficient available credit for said usage. Thus, if the user had a VDE node, the user might be able to use the traveling object if he had an appropriate, available budget available on his VDE node (and if necessary, allocated to him), and/or if he or his VDE node belonged to a specially authorized group of users or installations and/or if the traveling object carried its own budget(s). '193 patent at 131:59-132:18. **8(V)** VDE supports multiple differing hierarchies of client organization control information wherein an organization client administrator distributes control information specifying the usage rights of departments, users, and/or projects. Likewise, a department (division) network manager can function as a distributor (budgets, access rights, etc.) for department networks, projects, and/or users, etc. '193 patent at 33:63-34:3. **File Histories** **8(W)** Claims . . . are rejected under 35 U.S.C. 102(b) as being anticipated by Lofberg (4,595,950).

	Claim Term / Phrase	InterTrust Evidence
		The recited first device and its operation matches that of the rent terminal. . . . The information including at least one control is the personal identification information, see col. 3, lines 60-68 and col. 4, lines 64-68 and col. 13, lines 1-11. . . . The second device is the user station. The rent terminal determines whether the digital file may be copied and stored on the second device, see col. 9, lines 1-8 and col. 12, lines 43-49. The second device renders the digital file through its output only upon the data carrier having the information recorded therein and governing the use of the digital file is transferred to the second device. '193 Patent File History, 6/7/00 Office Action, p. 2. **8(X)** Claims . . . are rejected . . . as being anticipated by Karp (4,866,769). . . . The first device is a personal computer that is allowed access to the software by virtue of an encoded checkword derived from a source ID on the diskette and the personal computer ID, see Abstract. The information including at least one control is the list of checkwords stored in association with the digital file, see col. 5, line 60 through col. 6, line 11. A second device is represented by a second checkword stored in the list, see col. 8, lines 1-18. The determination of whether the digital file may be copied and stored by a second device is dependent on whether a checkword for the second device is allowed. '193 Patent File History, 6/7/00 Office Action, pp. 3-4. **8(Y)** Claims 58-59 are rejected . . . as being anticipated by Schull [5,509,070]. The Schull reference describes a system for distribution, registration and purchase of software. . . . The identified control is the need for a valid password to unlock the advanced features of the copied

	Claim Term / Phrase	InterTrust Evidence
		software. Column 7, line 10 through column 8, line 9 describe the generation and assignment of the target IDs and passwords. USP 5,915,019 File History, 7/28/97 Office Action, p. 3.
		8(Z) [Okano, 5,504,818] describes a system using cryptography for processing various digital objects. Figure 3 and column 6, line 33 disclose where a protected object may have embedded additional elements (security code attributes) to associate a control on the object. The control would restrict information according to security levels. USP 5,915,019 File History, 7/28/97 Office Action, p. 3.
		8(AA) A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. Figure 1 of Fischer shows various terminals connected via a communications channel 12. Terminal A, as a first apparatus recited in claim 7, includes user controls as per keyboard / crt, 4; communications port, see modem and communications channel 12; a processor as processor with main memory, 2.... '683 File History, 11/12/99 Office Action, p. 4.

	Claim Term / Phrase	InterTrust Evidence
9.	**controlling, control (v.)** 193.1, 861.58	**Patent Specifications** **9(A)** Secondary storage 652 in this example stores code and data used by CPU 654 and/or SPU 500 to control the overall operation of electronic appliance 600. '193 patent at 62:58-60. **9(B)** The other CPU(s) 654 may be any centrally controlling logic arrangement, such as for example, a microprocessor, other microcontroller, and/or array or other parallel processor. '193 patent at 64:55-58. **9(C)** A shared address/data bus arrangement 536 may transfer information between these various components under control of microprocessor 520 and/or DMA controller 526. '193 patent at 65:35-38. **9(D)** In some implementations, a separate arithmetic accelerator 544 may be omitted and any necessary calculations may be performed by microprocessor 520 under software control. '193 patent at 68:46-49. **9(E)** DMA controller 526 controls information transfers over address/data bus 536 without requiring microprocessor 520 to process each individual data transfer. '193 patent at 68:51-53.

	Claim Term / Phrase	InterTrust Evidence
		9(F) In the preferred embodiment, to control access to clearinghouses, users are assigned account numbers at clearinghouses. '193 patent at 268:29-31. --- **9(G)** . . . plural different control models regulating the use and/or auditing of either the same specific copy of electronic information content and/or differently regulating different copies (occurrences) of the same electronic information content. Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments. This includes supporting variable control information for budgeting and auditing usage as applied to a variety of predefined increments of electronic information, including employing a variety of different budgets and/or metering increments for a given electronic information deliverable for: billing units of measure, credit limit, security budget limit and security content metering increments, and/or market surveying and customer profiling content metering increments. '193 patent at 28:19-37. --- **9(H)** . . . support the flowing of content control information through different "branches" of content control information handling so as to accommodate, under the present invention's preferred embodiment, diverse controlled distributions of VDE controlled content. This allows different parties to employ the same initial electronic content with differing (perhaps competitive) control strategies. In this instance, a party who first placed control information on content can make certain control assumptions and these assumptions would evolve into more specific and/or extensive control assumptions. These control assumptions can evolve during the branching sequence upon content model participants submitting control information changes, for example, for use in "negotiating" with "in place" content control information. This can result in new or

	Claim Term / Phrase	InterTrust Evidence
		modified content control information and/or it might involve the selection of certain one or more already "in-place" content usage control methods over in-place alternative methods, as well as the submission of relevant control information parameter data. This form of evolution of different control information sets applied to different copies of the same electronic property content and/or appliance results from VDE control information flowing "down" through different branches in an overall pathway of handling and control and being modified differently as it diverges down these different pathway branches. '193 patent at 31:29-56. --- **9(I)** . . . multiple simultaneous control models for the same content property and/or property portion. This allows, for example, for concurrent business activities which are dependent on electronic commercial product content distribution, such as acquiring detailed market survey information and/or supporting advertising, both of which can increase revenue and result in lower content costs to users and greater value to content providers. Such control information and/or overall control models may be applied, as determined or allowed by control information, in differing manners to different participants in a pathway of content, reporting, payment, and/or related control information handling. VDE supports applying different content control information to the same and/or different content and/or appliance usage related activities, and/or to different parties in a content and/or appliance usage model, such that different parties (or classes of VDE users, for example) are subject to differing control information managing their use of electronic information content. For example, differing control models based on the category of a user as a distributor of a VDE controlled content object or an end-user of such content may result in different budgets being applied. Alternatively, for example, a one distributor may have the right to distribute a different array of properties than another distributor (from a common content collection provided, for example, on optical disc). An individual, and/or a class or other grouping of end-users, may have different costs (for example, a student, senior citizen, and/or poor citizen user of content who may be provided with the same or differing discounts) than a "typical" content user. '193 patent at 30:42-31:7.

	Claim Term / Phrase	InterTrust Evidence
		9(J) Such different application of control information may also result from content control information specifying that a certain party or group of parties shall be subject to content control information that differs from another party or group of parties. For example, content control information for a given piece of content may be stipulated as senior information and therefore not changeable, might be put in place by a content creator and might stipulate that national distributors of a given piece of their content may be permitted to make 100,000 copies per calendar quarter, so long as such copies are provided to bona fide end-users, but may pass only a single copy of such content to a local retailers and the control information limits such a retailer to making no more than 1,000 copies per month for retail sales to end-users. In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). '193 patent at 48:15-35. **9(K)** In this example, as illustrated in Figure 80, user B may receive control information associated with creator A's content from distributor A and/or user/distributor B. In either case, user B may be able to establish their own control information on DA(CA) and/or UDB(UDA(DA(CA))), respectively (if allowed by such control information. The resulting set(s) of control information, UB(DA(CA)) and/or UB(UDB(UDA(DA(CA)))) respectively, may represent different control scenarios, each of which may have benefits for user B. As described in connection with an earlier example, user B may have received control information from user/distributor B along a chain of handling including user/distributor A that bases fees on the number of minutes that user B makes use of creator A's content (and requiring user/distributor A to pay fees of $15 per month per user to distributor A regardless of the amount of usage by user B in a calendar month). This may be more favorable under some circumstances than the fees required by a direct use of control information provided by distributor A, but may also have the disadvantage of an exhausted chain of redistribution and, for example, further usage information reporting requirements included in UDB(UDA(DA(CA))). If the two sets of

	Claim Term / Phrase	InterTrust Evidence
		control information DA(CA) and UDB(UDA(DA(CA))) permit (e.g. do not require exclusivity enforced, for example, by using a registration interval in an object registry used by a secure subsystem of user B's VDE installation to prevent deregistration and reregistration of different sets of control information related to a certain container (or registration of plural copies of the same content having different control information and/or being supplied by different content providers) within a particular interval of time as an aspect of an extended agreement for a chain of handling and control reflected in DA(CA) and/or UDB(UDA(DA(CA)))), user B may have both sets of control information registered and may make use of the set that they find preferable under a given usage scenario. '193 patent at 306:30-65. **9(L)** For example, user/distributor A may receive control information CB that includes a requirement that user/distributor A pay creator B for content decrypted by user/distributor A (and any participant receiving distributed and/or redistributed control information from user/distributor A) at the rate of $0.50 per kilobyte. As indicated above, user/distributor A also may receive control information associated with creator B's VDE content container from distributor A. In this example, user/distributor A may have a choice between paying a "rental" fee through a chain of handling passing through distributor A, and a fee based on the quantity of decryption through a chain of handling direct to creator B. In this case, user/distributor A may have the ability to choose to use either or both of CB and DA(CB). '193 patent at 308:29-42. **9(M)** As illustrated in Figure 81, in this example, user B may receive control information associated with creator B's VDE content container from six different sources: CB directly from creator B, DA(CB) from distributor A, UDB(UDA(DA(CB))) and/or UDB(UDA(CB)) from user/distributor B, DC(CB) from distributor C, and/or DB(DC(CB)) from distributor B. This represents six chains of handling through which user B may enter into extended agreements with other participants in this example. Two of these

	Claim Term / Phrase	InterTrust Evidence
		chains pass through user/distributor B. Based on a VDE negotiation between user/distributor B and user B, an extended agreement may be reached (if permitted by control information governing both parties) that reflects the conditions under which user B may use one or both sets of control information. In this example, two chains of handling and control may "converge" at user/distributor B, and then pass to user B (and if control information permits, later diverge once again based on distribution and/or redistribution by user B). '193 patent at 308:48-65. --- **9(N)** User B may, in this example, receive a VDE content container from distributor C that is comprised of VDE objects created by creator B, creator C, and creator D. In addition, user B may receive a VDE content container from distributor B that contains the same content created by creator B, creator C, and creator D in addition to one or more extracted/embedded portions of content created by creator E. User B may base decisions concerning which of such containers they choose to use (including which embedded containers she may wish to use), and under which circumstances, based on, for example, the character of such extracted/embedded portions (e.g. multimedia presentations illustrating potential areas of interest in the remainder of the content, commentary explaining and/or expositing other elements of content, related works, improved application software delivered as an element of content, etc.); the quality, utility, and/or price (or other attributes of control information) of such portions; and other considerations which distinguish the containers and/or content control information received, in this example, from distributor B and distributor C. '193 patent at 312:11-31. --- **Extrinsic Sources** **9(O)** **control** *tr. v.* **-trolled, -trol-ling, -trols. 1.** To exercise authoritative or dominating influence over; direct. See Synonyms at **conduct. 2.** To hold in restraint; check: *struggled to control my temper; regulations intended to control prices.* **3. a.** To verify or regulate (a scientific experiment) by conducting a parallel

	Claim Term / Phrase	InterTrust Evidence
		experiment or by comparing with another standard. **b.** To verify (an account, for example) by using a duplicate register for comparison. –**control** *n.* **1.** Authority or ability to manage or direct: *lost control of the skidding car; the leaders in control of the country.* **2.** *Abbr.* **cont., contr. a.** One that controls; a controlling agent, device, or organization. **b.** Often **controls.** An instrument or set of instruments used to operate, regulate, or guide a machine or vehicle. **3.** A restraining device, measure, or limit; a curb: *a control on prices; price controls.* **4. a.** A standard of comparison for checking or verifying the results of an experiment. **b.** An individual or group used as a standard of comparison in a control experiment. **5.** An intelligence agent who supervises or instructs another agent. **6.** A spirit presumed to speak or act through a medium.[Middle English *controllen*, from Anglo-Norman *contreroller*, from Medieval Latin *contrarotulare*, to check by duplicate register, from *contrarotulus*, duplicate register : Latin *contra-*, contra- + Latin *rotulus*, roll, diminutive of *rota*, wheel. See ret-.]--**con-trol'la-bil'i-ty** *n.* --**con-trol'la-ble** *adj.* American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 410.

	Claim Term / Phrase	InterTrust Evidence
10.	**copy, copied, copying** 193.1, 193.11, 193.15, 193.19	**Patent Specifications** **10(A)** In some circumstances, a VDE administrator may require that a copy (partial or complete) of the back up files be transmitted to it within an administrative object to check for indications of fraudulent activities by the user. '193 patent at 167:63-67. **10(B)** When a user needs to access a particular VDE object 300, her electronic appliance 600 could issue a request over network 672 to obtain a copy of the object. The "VDE server" could deliver all or a portion of the requested object 300 in response to the request. '193 patent at 226:11-16. **10(C)** Expiration dates cannot be used effectively to prevent substitution of the previous copy of a budget UDE 1200. To secure these frequently updated items, a transaction tag is generated and included in the encrypted item each time that item is updated. '193 patent at 143:14-18. **10(D)** For example, author 3306A may have required that the repository encrypt each copy of shipped content using a different encryption key or keys in order to help maintain greater protection for content (e.g. in case an encryption key was "cracked" or inadvertently disclosed, the "damage" could be limited to the portion(s) of that specific copy of a certain content deliverable). '193 patent at 288:46-52.

	Claim Term / Phrase	InterTrust Evidence
		10(E) electronic testing will allow users to receive a copy (encrypted or unencrypted) of their test results when they leave the test sessions. '193 patent at 319:13-15. **10(F)** transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output, the portion of said digital file transferred to said second device representing a version of said digital file which, when rendered at said second device, provides a level of quality lower than the level of quality provided when said digital file is rendered at said first device; '193 patent at 323:64-324:4. **10(G)** For example, if the audit information received by the clearinghouse is legitimate, then the clearinghouse may send an administrative object to the end user's electronic appliance 600 requesting the electronic appliance to delete and/or compress the audit information that has been transferred. '193 patent at 162:10-15. **10(H)** [A] user (the "originating user") may wish to place an "originator controlled" ("ORCON") restriction on a certain document, such that the document may be transmitted and used only by those specific other users whom he designates (and only in certain, expressly authorized ways). Such a restriction may be flexible if the "distribution list" could be modified after the creation of the document, specifically in the event of someone requesting permission from the originating user to transmit the document outside the original list of authorized recipients. '193 patent at 278:11-21.

	Claim Term / Phrase	InterTrust Evidence
		10(I) Commercial content repository 200g may store content securely such that users may obtain such, when any required conditions are met, content from the repository 200g. The distribution permissions 3502 may, for example, permit commercial content repository 200g to create redistribution permissions and/or usage permissions 3500, 3502 using a VDE protected subsystem within certain restrictions described in content control information received from creator 102 (e.g., not to exceed a certain number of copies, requiring certain payments by commercial content repository 200g to creator 102, requiring recipients of such permissions to meet certain reporting requirements related to content usage information, etc.). Such content control information may be stored at the repository installation and be applied to unencrypted content as it is transmitted from said repository in response to a user request, wherein said content is placed into a VDE container as a step in a secure process of communicating such content to a user. '193 patent at 316:16-37. **10(J)** 37. A method as in claim 36, further comprising: at some point after said transferring step, taking at least one action to render said copy of said first digital file unuseable at said second device; and at said first digital device, removing said encumbrance on said budget, said removal including increasing the number of copies of said first digital file authorized by said budget. '193 patent at 325:32-40. **Extrinsic Sources** **10(K)** **copy** To reproduce data in a new location or other destination, leaving the source data unchanged, although the physical form of

	Claim Term / Phrase	InterTrust Evidence
		the result may differ from that of the source; for example, to make a duplicate of all the programs or data on a disk, or to copy a graphic screen image to a printer. Spencer, Personal Computer Dictionary (Camelot Publishing, 1995), p. 47. **10(L)** **copy** 1. The material, including text, graphic images, pictures, and artwork, to be assembled for printing. To reproduce part of a document at another location in the document or in another document. Webster's New World Dictionary of Computer Terms, 6th ed. (1997), p. 118. **10(M)** **copy** *n., pl.* **–ies. 1.** An imitation or reproduction of an original; a duplicate: *a copy of a painting; made two copies of the letter.* **2.** One specimen or example of a printed text or picture: *an autographed copy of a novel.* **3.** *Abbr.* **c., C.** Material, such as a manuscript, that is to be set in type. **4.** The words to be printed or spoken in an advertisement. **5.** Suitable source material for journalism: *Celebrities make good copy.* **–copy** *v.* **-ied, -ying, -ies** *–tr.* **1.** To make a reproduction or copy of. **2.** To follow as a model or pattern; imitate. See Synonyms at **imitate.** *–intr.* **1.** To make a copy or copies. **2.** To admit of being copied: *colored ink that does not copy well.* American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 416.

	Claim Term / Phrase	InterTrust Evidence
11.	**derive** 900.155	**Patent Specifications** **11(A)** Whenever CPU/SPU 2650 enters or leaves the "SPU" mode, the transition is performed in such a way that no information contained in the secure memory 532, 534 or derived from it (e.g., stored in registers or a cache memory associated with microprocessor 2652) while in the "SPU" mode can be exposed by microprocessor 2652 operations that occur in the "normal" mode. '900 patent at 75:30-36. **11(B)** In some example implementations, interrupts may be enabled while CPU/SPU 2650 is operating in the "SPU" mode similarly interrupts and returns from interrupts while in the "SPU" mode may allow transitions from "SPU" mode to "normal" mode and back to "SPU" mode without exposing the content of secure memory 532, 534 or the content of registers or other memory associated with microprocessor 2652 that may contain information derived from secure mode operation. '900 patent at 75:41-49. **11(C)** For example, during PPE 650 operation, the internal state of the PPE is constantly being updated. During each interaction with a trusted server, PPE 650 (and the trusted server) may test the internal state of PPE 650 to determine whether it could be derived from the internal state last seen by the trusted server for this particular PPE 650 instance. If it could not, the result may be taken as indicating a replay attack of some sort, and an appropriate action can be taken (see Figure 69L, block 3592, 3594, 3596). '900 patent at 247:4-12. **11(D)** For example, the counter could be repeated hashing (e.g., with

	Claim Term / Phrase	InterTrust Evidence
		MD5) of a value that is stored redundantly in several different locations within the operational materials 3472 and secure database 610 - so that the trusted server could verify that the current value can be derived (e.g., by repeated MD5 applications) from a previous value. '900 patent at 247:20-26. --- **Extrinsic Sources** **11(E)** **derive**: *v.* **de-rived, de-riv-ing, de-rives.** *v. tr.* **1.** To obtain or receive from a source. **2.** To arrive at by reasoning; deduce or infer: *derive a conclusion from facts.* **3.** To trace the origin or development of (a word). **4.** *Chemistry.* To produce or obtain (a compound) from another substance by chemical reaction.v. intr. To issue from a source; originate. See Synonyms at **stem1**.[Middle English *deriven*, to be derived from, from Old French *deriver*, from Latin *derivare*, to derive, draw off : *de-*, de- + *rivus*, stream. See rei-.]--**de-riv'a-ble** *adj.* --**de-riv'er** *n.* American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 504.

	Claim Term / Phrase	InterTrust Evidence
12.	**designating** 721.1	**Patent Specifications** **12(A)** Figures 11A-11C show how a verifying authority can use different digital signatures to designate the same or different load modules as being appropriate for execution by different assurance level electronic appliances; '721 patent at 7:66-8:2. **12(B)** In one of its roles or instances, object submittal manager 774 provides a user interface 774a that allows the user to create an object configuration file 1240 specifying certain characteristics of a VDE object 300 to be created. This user interface 774a may, for example, allow the user to specify that she wants to create an object, allow the user to designate the content the object will contain, and allow the user to specify certain other aspects of the information to be contained within the object (e.g., rules and control information, identifying information, etc.). '193 patent at 103:11-20. **12(C)** Control sets 914 exist in two types in VDE 100: common required control sets which are given designations "control set 0" or "control set for right," and a set of control set options. '193 patent at 150:30-33. **12(D)** The classification attributes may designate the overall level of sensitivity of the document as an element of an ordered set. For example, the set "unclassified," "confidential," "secret," "top secret" might be appropriate in a government setting, and the set "public," "internal," "confidential," "registered confidential" might be appropriate in a corporate setting.

	Claim Term / Phrase	InterTrust Evidence
		The compartment attributes may designate the document's association with one or more specific activities within the organization, such as departmental subdivisions (e.g., "research," "development," "marketing") or specific projects within the organization. Each person using an electronic appliance 600 would be assigned, by an authorized user, a set of permitted sensitivity attributes to designate those documents, or one or more portions of certain document types, which could be processed in certain one or more ways, by the person's electronic appliance. A document's sensitivity attribute would have to belong to the user's set of permitted sensitivity values to be accessible. In addition, the organization may desire to permit users to exercise control over specific documents for which the user has some defined responsibility. As an example, a user (the "originating user") may wish to place an "originator controlled" ("ORCON") restriction on a certain document, such that the document may be transmitted and used only by those specific other users whom he designates (and only in certain, expressly authorized ways). '193 patent at 277:56-278:16. **12(E)** A document may have an attribute designating its originator and requiring an explicit permission to be granted by an originator before the document's content could be viewed. '193 patent at 280:1-4. **Extrinsic Sources** **12(F)** **designate** *tr. v.* **–nated, -nating, -nates. (1)** To indicate or specify; point out. **(2)** To give a name or title to; characterize. **(3)** To select and set aside for a duty, an office, or a purpose. See Synonyms at **allocate, appoint.** American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 506.

	Claim Term / Phrase	InterTrust Evidence
13.	device class 721.1	<u>File Histories</u> 13(A) . . . Applicants respectfully submit that some of the terms cited by the Examiner as "indefinite" are either well-known by persons skilled in the art or inherently clear. For example . . . the term "class" is used as part of the phrase "device class." Applicants respectfully submit that "device class" is inherently clear, meaning a group of devices which share at least one attribute. '721 Patent File History, 4/13/99 Response, p. 14.

	Claim Term / Phrase	InterTrust Evidence
14.	**digital signature, digitally signing** 721.1	**Patent Specifications** **14(A)** A verifying authority digitally "signs" and "certifies" those load modules or other executables it has verified (using a public key based digital signature and/or certificate based thereon, for example). Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. '721 patent at 4:64-5:5. --- **14(B)** In accordance with another aspect provided by the present invention, an execution environment protects itself by deciding — based on digital signatures, for example — which load modules or other executables it is willing to execute. A digital signature allows the execution environment to test both the authenticity and the integrity of the load module or other executables, as well permitting a user of such executables to determine their correctness with respect to their associated specifications or other description of their behavior, if such descriptions are included in the verification process. '721 patent at 6:5-15. --- **14(C)** A verifying authority may digitally sign load modules or other executables with a digital signature that indicates or implies assurance level. A verifying authority can use digital signature techniques to distinguish between assurance levels. As one example, each different digital signature may be encrypted using a different verification key and/or fundamentally different encryption, one-way hash and/or other techniques. A protected processing environment or other secure execution space protects itself by

	Claim Term / Phrase	InterTrust Evidence
		executing only those load modules or other executables that have been digitally signed for its corresponding assurance level. '721 patent at 6:42-52. **14(D)** Figure 5 shows how a verifying authority can create a certifying digital signature Figure 6 shows how a protected processing environment can securely authenticate a verifying authority's digital signature to guarantee the integrity of the corresponding load module; Figure 7 shows how several different digital signatures can be applied to the same load module; Figure 8 shows how a load module can be distributed with multiple digital signatures '721 patent at 7:47-57. **14(E)** The two digital signature algorithms in widespread use today (RSA and DSA) are based on distinct mathematical problems (factoring in the case of RSA, discrete logs for DSA). '721 patent at 15:31-34. **14(F)** There exist many well known processes for creating digital signatures. One example is the Digital Signature Algorithm (DSA). DSA uses a public-key signature scheme that performs a pair of transformations to generate and verify a digital value called a "signature." '721 patent at 10:60-64.

	Claim Term / Phrase	InterTrust Evidence
		Extrinsic Sources **14(G)** **digital signature**. In data security, a data block appended to a message, or a complete encrypted message, such that the recipient can authenticate the message contents and/or prove that it could only have originated with the purported sender. The digital signature is a function of: (a) the message, transaction or document to be signed; (b) secret information known only to the sender; and (c) public information employed in the validation process. Message authentication enables the receiver of a message to ensure that the contents cannot be changed accidentally or deliberately by a third party. However, since both the sender and the receiver share the same secret information there is no method of resolving disputes. The receiver can compute the authenticator and could therefore change a message, or forge a new message, develop the authenticator and claim that it was transmitted by the sender sharing the same secret key for authentication. Conversely the sender could disown an authenticated message and claim that the receiver produced a forged message using the common secret key. The essence of a digital signature is that the receiver must be able to prove that a message originated with a given sender, but must not be able to construct the signed message. Thus the sender requires secret information to construct the signed message and the receiver must be able to access public information for use in the validation of the message. In the case of a dispute the receiver must be in a position to supply non-secret information to a judge (i.e., the signed message and the publicly available information) in order to prove the authentication and origin of the message. *Compare* DYNAMIC PASSWORD. *See* MESSAGE AUTHENTICATION, PUBLIC KEY CRYPTOGRAPHY, RSA. *Synonymous with* ELECTRONIC SIGNATURE. Dictionary of Information Technology, 3d ed. (Van Nostrand Reinhold, 1989), pp. 160-161. --- **Citations from Sources Designated by Microsoft under PLR 4-2(b)** **14(H)** **Digital signature** A string of characters that can be generated only by an agent that knows some secret, and hence provides evidence

	Claim Term / Phrase	InterTrust Evidence
		that such an agent must have generated it. Neumann, Computer Related Risks (ACM Press, 1995), p. 345.
		14(I) Another way to check your files for unauthorized tampering is to derive a signature for each file, and to compare that signature against a known value. A file signature is a function of the contents and properties of the file. A signature is relatively easy to calculate, but difficult to forge. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), p. 122.

	Claim Term / Phrase	InterTrust Evidence
15.	**executable, executable programming** 721.34, 912.8, 912.35	**Patent Specifications** **15(A)** The next section of load module 1100 is an encrypted executable body 1106 that contains one or more blocks of encrypted code. Load modules 1100 are preferably coded in the "native" instruction set of their execution environment for efficiency and compactness. SPU 500 and platform providers may provide versions of the standard load modules 1100 in order to make their products cooperate with the content in distribution mechanisms contemplated by VDE 100. The preferred embodiment creates and uses native mode load modules 1100 in lieu of an interpreted or "p-code" solution to optimize the performance of a limited resource SPU. However, when sufficient SPE (or HPE) resources exist and/or platforms have sufficient resources, these other implementation approaches may improve the cross platform utility of load module code. '193 patent at 141:42-56. --- **15(B)** The load module or other executable is preferably constructed using a programming language (e.g., languages such as Java and Python) and/or design/implementation methodology (e.g., Gypsy, FDM) that can facilitate automated analysis, validation, verification, inspection, and/or testing. '721 patent at 5:34-39. --- **Extrinsic Sources** **15(C)** **executable** *adj.* Of, pertaining to, or being a program file that can be run. Executable files have extensions such as .bat, .com, and .exe. **executable** *n.* A program file that can be run, such as file0.bat, file1.exe, or file2.com. **executable program** *n.* A program that can be run. The term

	Claim Term / Phrase	InterTrust Evidence
		usually applies to a compiled program translated into machine code in a format that can be loaded into memory and run by a computer's processor. In interpreter languages, an executable program can be source code in the proper format. *See also* code (definition 1), compiler (definition 2), computer program, interpreter, source code. Microsoft Computer Dictionary, 3d ed. (Microsoft Press, 1997), p. 182.

	Claim Term / Phrase	InterTrust Evidence
16.	**host processing environment** 900.155	**Patent Specifications** **16(A)** Personal computer 4116 in this example is also provided with a secure processing unit 500 or software based HPE 655 (See Figure 12) to provide secure, tamper-resistant trusted processing. '683 patent at 20:16-19. --- **16(B)** "Protected Processing Environment" ("PPE") 650 may refer generally to SPE 503 and/or HPE 655. Hereinafter, unless context indicates otherwise, references to any of "PPE 650," "HPE 655" and "SPE 503" may refer to each of them. '193 patent at 105:18-22; '900 patent at 112:48-52. --- **16(C)** As discussed above in connection with Figure 12, each electronic appliance 600 in the preferred embodiment includes one or more SPEs 503 and/or one or more HPEs 655. These secure processing environments each provide a protected execution space for performing tasks in a secure manner. They may fulfill service requests passed to them by ROS 602, and they may themselves generate service requests to be satisfied by other services within ROS 602 or by services provided by another VDE electronic appliance 600 or computer. In the preferred embodiment, an SPE 503 is supported by the hardware resources of an SPU 500. An HPE 655 may be supported by general purpose processor resources and rely on software techniques for security protection. HPE 655 thus gives ROS 602 the capability of assembling and executing certain component assemblies 690 on a general purpose CPU such as a microcomputer, minicomputer, mainframe computer or supercomputer processor. In the preferred embodiment, the overall software architecture of an SPE 503 may be the same as the software architecture of an HPE 655. An HPE 655 can "emulate" SPE 503 and associated SPU 500, i.e., each may include services and resources needed to support an identical set of service requests from ROS 602 (although ROS 602

	Claim Term / Phrase	InterTrust Evidence
		may be restricted from sending to an HPE certain highly secure tasks to be executed only within an SPU 500). '193 patent at 104:39-64; '900 patent at 112:2-27.
		16(D) In the preferred embodiment, HPE 655 is a secure processing environment supported by a processor other than an SPU, such as for example an electronic appliance CPU 654 general-purpose microprocessor or other processing system or device. In the preferred embodiment, HPE 655 may be considered to "emulate" an SPU 500 in the sense that it may use software to provide some or all of the processing resources provided in hardware and/or firmware by an SPU. HPE 655 in one preferred embodiment of the present invention is full-featured and fully compatible with SPE 503—that is, HPE 655 can handle each and every service call SPE 503 can handle such that the SPE and the HPE are "plug compatible" from an outside interface standpoint (with the exception that the HPE may not provide as much security as the SPE). '193 patent at 79:60-80:7; '900 patent at 87:32-46.
		16(E) Figure 12 also shows that ROS 602 may provide one or more SPEs 503 and/or one or more HPEs 655. As discussed above, HPE 655 may "emulate" an SPU 500 device, and such HPEs 655 may be integrated in lieu of (or in addition to) physical SPUs 500 for systems that need higher throughput. Some security may be lost since HPEs 655 are typically protected by operating system security and may not provide truly secure processing. Thus, in the preferred embodiment, for high security applications at least, all secure processing should take place within an SPE 503 having an execution space within a physical SPU 500 rather than a HPE 655 using software operating elsewhere in electronic appliance 600. '193 patent at 88:31-43; '900 patent at 96:6-18.
		16(F) Occurrence of the control operation demonstrates that

	Claim Term / Phrase	InterTrust Evidence
		microprocessor 2652 is executing in its most privileged "normal" mode and therefore can be trusted to execute successfully the "enter 'SPU' mode" sequence of instructions stored in secure memory 532. If microprocessor 2652 were not executing in its most privileged mode, there would be no assurance that those instructions would execute successfully. Because switch 2663 isolates microprocessor 2652 from external signals (e.g., interrupts) until "SPU" mode is successfully initialized, the entry instructions can be guaranteed to complete successfully. '900 patent at 78:30-40. **16(G)** Designing VDE capabilities into one or more standard microprocessor, microcontroller and/or other digital processing components may materially reduce VDE related hardware costs by employing the same hardware resources for both the transaction management uses contemplated by the present invention and for other, host electronic appliance functions. This means that a VDE SPU can employ (share) circuitry elements of a "standard" CPU. For example, if a "standard" processor can operate in protected mode and can execute VDE related instructions as a protected activity, then such an embodiment may provide sufficient hardware security for a variety of applications and the expense of a special purpose processor might be avoided. Under one preferred embodiment of the present invention, certain memory (e.g., RAM, ROM, NVRAM) is maintained during VDE related instruction processing in a protected mode (for example, as supported by protected mode microprocessors). '193 patent at 21:5-21; '900 patent at 21:1-17. **16(H)** A VDE node's hardware SPU is a core component of a VDE secure subsystem and may employ some or all of an electronic appliance's primary control logic, such as a microcontroller, microcomputer or other CPU arrangement. This primary control logic may be otherwise employed for non VDE purposes such as the control of some or all of an electronic appliance's non-VDE functions. When operating in a hardware SPU mode, said primary control logic must be sufficiently secure so as to protect and conceal important VDE

	Claim Term / Phrase	InterTrust Evidence
		processes. For example, a hardware SPU may employ a host electronic appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute with a certain degree of security. This alternate embodiment is in contrast to the preferred embodiment wherein a trusted environment is created using a combination of one or more tamper resistant semiconductors that are not part of said primary control logic. '193 patent at 49:33-50; '900 patent at 49:31-48.

	Claim Term / Phrase	InterTrust Evidence
17.	**identifier** 193.15, 912.8	**Patent Specifications** **17(A)** This same termination (or other specified consequence such as budget reduction, price increase, message displays on screen to users, messages to administrators, etc.) can also be the consequence of the failure by a user or the users VDE installation to complete a monitored process, such as paying for usage in electronic currency, failure to perform backups of important stored information (e.g., content and/or appliance usage information, control information, etc.), failure to use a repeated failure to use the proper passwords or other identifiers, etc.). '193 patent at 270:12-21 **17(B)** During the same or different communication session, the terminal could similarly, securely communicate back to the portable appliance 2600 VDE secure subsystem details as to the retail transaction (for example, what was purchased and price, the retail establishment's digital signature, the retail terminal's identifier, tax related information, etc.). '193 patent at 233:35-41. **17(C)** Many load modules 1100 contain code that executes in an SPE 503. Some load modules 1100 contain code that executes in an HPE 655. This allows methods 1000 to execute in whichever environment is appropriate. For example, an INFORMATION method 1000 can be built to execute only in SPE 503 secure space for government classes of security, or in an HPE 655 for commercial applications. As described above, the load module public header 802 may contain an "execution space code" field that indicates where the load module 1100 needs to execute. This functionality also allows for different SPE instruction sets as well as different user platforms, and allows methods to be constructed without dependencies on the underlying load module instruction set. '193 patent at 140:37-50.

	Claim Term / Phrase	InterTrust Evidence
		17(D) [VDE features] provide very flexible and extensible user identification according to individuals, installations, by groups such as classes, and by function and hierarchical identification employing a hierarchy of levels of client identification (for example, client organization ID, client department ID, client network ID, client project ID, and client employee ID, or any appropriate subset of the above). '193 patent at 25:31-38. **17(E)** Account Numbers and User IDs In the preferred embodiment, to control access to clearinghouses, users are assigned account numbers at clearinghouses. Account numbers provide a unique "instance" value for a secure database record from the point of view of an outsider. From the point of view of an electronic appliance 600 site, the user, group, or group/user ids provide the unique instance of a record. For example, from the point of view of VISA, your Gold Card belongs to account number #123456789. From the point of view of the electronic appliance site (for example, a server at a corporation), the Gold card might belong to user id 1023. In organizations which have plural users and/or user groups using a VDE node, such users and/or user groups will likely be assigned unique user IDs. '193 patent at 268:28-42. **Extrinsic Sources** **17(F)** **identify** v. **identified, identifying, identifies.** v. tr. **1.** To establish the identity of. **2.** To ascertain the origin, nature, or definitive characteristics of. **3.** *Biology.* To determine the taxonomic classification of (an organism). **4.** To consider as identical or united; equate. **5.** To associate or affiliate (oneself) closely with a person or group.v. intr. To establish an identification with another or others.[Medieval Latin *identificare*, to make to resemble : Late Latin *identitas*, identity. See IDENTITY + Latin *-ficare*, -fy.]**--i-den'ti-fi'a-ble** *adj.* **--i-den'ti-fi'a-bly** *adv.* **--i-den'ti-fi'er** *n.* American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 896.

	Claim Term / Phrase	InterTrust Evidence
18.	**protected processing environment** 683.2, 721.34	**Patent Specifications** **18(A)** Because security may be better/more effectively enforced with the assistance of hardware security features such as those provided by SPU 500 (and because of other factors such as increased performance provided by special purpose circuitry within SPU 500), at least one SPE 503 is preferred for many or most higher security applications. However, in applications where lesser security can be tolerated and/or the cost of an SPU 500 cannot be tolerated, the SPE 503 may be omitted and all secure processing may instead be performed by one or more secure HPEs 655 executing on general purpose CPUs 654. '193 patent 80:65-81:8. **18(B)** The Ginter et al. patent disclosure describes, among other things, techniques for providing a secure, tamper resistant execution spaces within a "protected processing environment" for computer programs and data. The protected processing environment described in Ginter et al. may be hardware-based, software-based, or a hybrid. '721 patent 3:16-21. **18(C)** One particular example of a secure execution space is a "protected processing environment" 108 of the type shown in Ginter et al. (see Figures 6-12) and described in associated text. Protected processing environments 108 provide a secure execution environment in which appliances 58, 60, 62 may securely execute load modules 54 to perform useful tasks. '721 patent 8:33-40. **18(D)** In this example, appliance 600 may include one or more processors 4126 providing or supporting one or more "protected processing

	Claim Term / Phrase	InterTrust Evidence
		environments" (PPE) 650 (e.g., SPEs 503 and/or HPEs 544) shown in Figures 6-12 and 62-72). Protected processing environment 650 may, for example, be implemented using a secure processing unit (SPU) 500 of the type shown in Figure 9 and/or may be based on software tamper-resistance techniques or a combination of software and hardware. As described above in detail, protected processing environment 650 provides a secure, trusted environment for storing, manipulating, executing, modifying and otherwise processing secure information such as that provided in secure electronic containers 302. In this particular example, secure containers 302 may not be opened except within a protected processing environment 650. Protected processing environment 650 is provided with the cryptographic and other information it needs to open and manipulate secure containers 302, and is tamper resistant so that an attacker cannot easily obtain and use this necessary information. '683 patent 29:51-30:3. **18(E)** Figure 10 is a block diagram of one example of a software structure/architecture for Rights Operating System ("ROS") 602 provided by the preferred embodiment. In this example, ROS 602 includes an operating system ("OS") "core" 679, a user Application Program Interface ("API") 682, a "redirector" 684, an "intercept" 692, a User Notification/Exception Interface 686, and a file system 687. ROS 602 in this example also includes one or more Host Event Processing Environments ("HPEs") 655 and/or one or more Secure Event Processing Environments ("SPEs") 503 (these environments may be generically referred to as "Protected Processing Environments" 650). HPE(s) 655 and SPE(s) 503 are self-contained computing and processing environments that may include their own operating system kernel 688 including code and data processing resources. A given electronic appliance 600 may include any number of SPE(s) 503 and/or any number of HPE(s) 655. HPE(s) 655 and SPE(s) 503 may process information in a secure way, and provide secure processing support for ROS 602. For example, they may each perform secure processing based on one or more VDE component assemblies 690, and they may each offer secure processing services to OS kernel 680. In the preferred embodiment, SPE 503 is a secure processing environment provided at least in part by an SPU 500. Thus, SPU

	Claim Term / Phrase	InterTrust Evidence
		500 provides the hardware tamper-resistant barrier 503 surrounding SPE 503. SPE 503 provided by the preferred embodiment is preferably: small and compact loadable into resource constrained environments such as for example minimally configured SPUs 500 dynamically updatable extensible by authorized users integratable into object or procedural environments secure. In the preferred embodiment, HPE 655 is a secure processing environment supported by a processor other than an SPU, such as for example an electronic appliance CPU 654 general-purpose microprocessor or other processing system or device. In the preferred embodiment, HPE 655 may be considered to "emulate" an SPU 500 in the sense that it may use software to provide some or all of the processing resources provided in hardware and/or firmware by an SPU. HPE 655 in one preferred embodiment of the present invention is full-featured and fully compatible with SPE 503—that is, HPE 655 can handle each and every service call SPE 503 can handle such that the SPE and the HPE are "plug compatible" from an outside interface standpoint (with the exception that the HPE may not provide as much security as the SPE). HPEs 655 may be provided in two types: secure and not secure. For example, it may be desirable to provide non-secure versions of HPE 655 to allow electronic appliance 600 to efficiently run non-sensitive VDE tasks using the full resources of a fast general purpose processor or computer. Such non-secure versions of HPE 655 may run under supervision of an instance of ROS 602 that also includes an SPE 503. In this way, ROS 602 may run all secure processes within SPE 503, and only use HPE 655 for processes that do not require security but that may require (or run more efficiently) under potentially greater resources provided by a general purpose computer or processor supporting HPE 655. Non-secure and secure HPE 655 may operate together with a secure SPE 503. '193 patent 79:24-80:21.
		18(F) Figure 13 shows the software architecture of the preferred embodiment Secure Processing Environment (SPE) 503. This

	Claim Term / Phrase	InterTrust Evidence
		architecture may also apply to the preferred embodiment Host Processing Environment (HPE) 655. "Protected Processing Environment" ("PPE") 650 may refer generally to SPE 503 and/or HPE 655. '193 patent 105:15-20. **18(G)** In some embodiments and where commercially acceptable, certain VDE participants, such as clearinghouses that normally maintain sufficiently physically secure non-VDE processing environments, may be allowed to employ HPEs rather VDE hardware elements and interoperate, for example, with VDE end-users and content providers. '193 patent 13:17-23. **18(H)** An end user may make use of credit and/or currency securely stored within the end user's VDE installation secure subsystem to pay for charges related to use of VDE content received from the repository, and/or the user may maintain a secure credit and/or currency account remotely at the repository, including a "virtual" repository where payment is made for the receipt of such content by an end user. This later approach may provide greater assurance for payment to the repository and/or content providers particularly if the end user has only an HPE based secure subsystem. '193 patent 291:39-49. **18(I)** One way to inexpensively and conveniently deploy multiple instances of VDE electronic appliances 600 across a network would be to provide network workstations with software defining an HPE 655. This arrangement requires no hardware modification of the workstations; an HPE 655 can be defined using software only. An SPE(s) 503 and/or HPE(s) 655 could also be provided within a VDE server. This arrangement has the advantage of allowing distributed VDE network processing without requiring workstations to be

	Claim Term / Phrase	InterTrust Evidence
		customized or modified (except for loading a new program(s) into them). VDE functions requiring high levels of security may be restricted to an SPU-based VDE server. "Secure" HPE-based workstations could perform VDE functions requiring less security, and could also coordinate their activities with the VDE server. '193 patent 226:43-57.
		18(J) Large Organization Example In a somewhat more general example, suppose an organization (e.g., a corporation or government department) with thousands of employees and numerous offices disposed throughout a large geographic area wishes to exercise control over distribution of information which belongs to said organization (or association). '193 patent 277:26-32.
		18(K) User Environment In an organization (or association) such as that described above, users may utilize a variety of electronic appliances 600 for processing and managing documents. This may include personal computers, both networked and otherwise, powerful single-user workstations, and servers or mainframe computers. To provide support for the control information described in this example, each electronic appliance that participates in use and management of VDE-protected documents may be enhanced with a VDE secure subsystem supporting an SPE 503 and/or HPE 655. In some organizations, where the threats to secure operation are relatively low, an HPE 655 may suffice. In other organizations (e.g., government defense), it may be necessary to employ an SPE 503 in all situations where VDE-protected documents are processed. The choice of enhancement environment and technology may be different in different of the organization. Even if different types of PPE 650 are used within an organization to serve different

	Claim Term / Phrase	InterTrust Evidence
		requirements, they may be compatible and may operate on the same types (or subsets of types) of documents. '193 patent 278:45-65.
		18(L) This manufacturing process may include, [redacted], testing the bootstrap loader and challenge-response software permanently stored within PPE 650, and [redacted] '193 patent 223:36-39.
		18(M) [redacted] '193 patent at 49:59-62.
		18(N) [redacted] '193 patent at 221:2-6.
		18(O) VDE 100 provided by the preferred embodiment has [redacted] security to help ensure that it cannot be compromised [redacted] successful "brute force attack," and so that the time and cost to succeed in such a "brute force attack" substantially exceeds any value to be derived. In addition, the security provided by VDE 100 compartmentalizes the internal workings of VDE so that [redacted]

	Claim Term / Phrase	InterTrust Evidence
		bounded subset of protected information, not the entire system. '193 patent at 199:38-46.
		18(P) VDE supports trusted (sufficiently secure) electronic information distribution and usage control models for both commercial electronic content distribution and data security applications. '193 patent at 16:25-28.
		18(Q) 1. A security method comprising: (a) digitally signing a first load module with a first digital signature designating the first load module for use by a first device class; (b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class; (c) distributing the first load module for use by at least one device in the first device class; and (d) distributing the second load module for use by at least one device in the second device class. '721 patent at 21:9-24.
		18(R) 34. A protected processing environment comprising: a first tamper resistant barrier having a first security level, a first secure execution space, and

	Claim Term / Phrase	InterTrust Evidence
		at least one arrangement within the first tamper resistant barrier that prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level. '721 patent at 24:48-56. **18(S)** [VDE features] support security techniques that materially increase the time required to "break" a system's integrity. This includes using a collection of techniques that minimizes the damage resulting from comprising some aspect of the security features of the present inventions. '193 patent at 35:59-63. **18(T)** Fingerprinting electronic content before it is encrypted for transfer to a customer or other user provides information that can be very useful for identifying who received certain content which may have then been distributed or made available in unencrypted form. This information would be useful in tracking who may have "broken" the security of a VDE installation and was illegally making certain electronic content available to others. '193 patent at 38:4-12. **18(U)** If a content key becomes compromised, the portion of the content encrypted with the key is also compromised until the key "ages" and expires. If the "aging" process for that key also becomes compromised, then the breach becomes permanent. '193 patent at 222:49-53.

	Claim Term / Phrase	InterTrust Evidence
		18(V) If PPE 650 (or a VDE administrator watching its activities or communicating with it) detects that it has been compromised, it may be updated with an initialization to use new code, keys and new encryption/decryption algorithms. This would limit exposure to VDE objects 300 that existed at the time the encryption scheme was broken. '193 patent at 223:4-10. **18(W)** Secure VDE hardware (also known as SPUs for Secure Processing Units), or VDE installations that use software to substitute for, or complement, said hardware (provided by Host Processing Environments (HPEs)), operate in conjunction with secure communications, systems integration software, and distributed software control information and support structures, to achieve the electronic contract/rights protection environment of the present invention. '193 patent at 13:7-14. **File Histories** **18(X)** . . . the Examiner objects to the use of "environment" as indefinite and unclear. This word, however, is not used in isolation, but rather in the context of several longer phrases, all of which are defined in the specification. The phrase "protected processing environment," for example, is . . . described on at least, for example, pages 7-8 and 25 of the specification. . . . These terms are also described in the commonly assigned copending application . . . filed 13 February 1995. '721 Patent File History, 4/13/99 Amendment, p. 13.

	Claim Term / Phrase	InterTrust Evidence
		Citations from Sources Designated by Microsoft under PLR 4-2(b) **18(Y)** Furthermore, there is never an absolute sense in which a system is secure or reliable. Neumann, Computer Related Risks (ACM Press, 1995), p. 2. --- **18(Z)** The fundamental purpose of security is to minimize the risk of loss from (1) physical damage or destruction, (2) human errors and omissions, and (3) theft or unauthorized disclosure. That purpose is best fulfilled by effective loss-prevention efforts. Loss-prevention efforts involve the identification and assessment of risks to capital, human, informational, and technological assets, and the development of suitable and cost-feasible countermeasures. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 75. --- **18(AA)** Total software security is no more attainable than is perfect security in any other area. A highly skilled programmer can almost always penetrate software safeguards written by another programmer. Of course, the same can be said for attorneys; an unprincipled lawyer can usually get around protections in a contract written by an-other lawyer. Yet contracts continue to be written, and, for the most part, they are effective. Computer software security routines can also be effective most of the time. A security procedure does not have to be all-encompassing. If it provides reasonable protection at an acceptable cost, it is certainly worthwhile. The basic consideration is one of degree—how important are specific elements of data and software, and how important is their security. Some data require very little security. For example, a software library containing programs that are similar to those found in many other computer installations does not require elaborate security protection against theft. On the other hand, proprietary programs and sensitive data require extensive

	Claim Term / Phrase	InterTrust Evidence
		security. A data base containing payroll information requires stringent security procedures to maintain its confidentiality. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 201.
		18(BB) Regardless of which form of data storage is being considered, one must bear in mind a vital concept: no data processing installation can afford 100 percent security—if indeed there is such a thing. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 218.
		18(CC) One hundred percent security cannot be achieved. The most effective systems apply security protection techniques in layers. Each layer of protection diminishes the chances of someone breaking through the barriers. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), pp. 293.
		18(DD) Risk analysis is not intended to come up with a plan for absolute security. Indeed, absolute security is not achievable in today's computer's systems. Rather, risk analysis produces a degree of security commensurate with the information to be protected and with the amount of resources to be expended. Hoffman, Modern Methods for Computer Security and Privacy (Prentice-Hall, 1977), p. 170.
		18(EE) No matter how secure you make them, computers can always be broken into given sufficient resources, time, and money. Computers are especially vulnerable because software is complex and we don't always know if there are flaws present that make the task of breaking in easier. Even systems that are certified according to the

	Claim Term / Phrase	InterTrust Evidence
		Department of Defense's so-called Orange Book are vulnerable, especially if they are not administered correctly. Just as six-foot-thick vaults doors don't work if they're not administered properly. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), pp. 13.
		18(FF) Security is a relative, not an absolute, concept, and gains in security often come only with penalties in performance. Landwehr, Formal Models for Computer Security, ACM Computer Surveys (Sept. 3, 1981), p. 253.

	Claim Term / Phrase	InterTrust Evidence
19.	**secure, securely** 193.1, 193.11, 193.15, 861.58, 891.1, 683.2, 721.34, 912.8, 912.35	**Patent Specifications** **19(A)** VDE normally employs an integration of cryptographic and other security technologies (e.g. encryption, digital signatures, etc.), with other technologies . . . . '193 patent 8:1-3. **19(B)** Since VDE also employs secure (e.g. encrypted and authenticated) communications when passing information between the participant location (nodes) secure subsystems of a VDE arrangement, important components of a VDE electronic agreement can be reliably enforced with sufficient security (sufficiently trusted) for the intended commercial purposes. '193 patent 45:39-45. **19(C)** The degree of overall security of the VDE system is primarily dependent on the degree of tamper resistance and concealment of VDE control process execution and related data storage activities. '193 patent 21:26-29. **19(D)** Because of the VDE security, including use of effective encryption, authentication, digital signaturing, and secure database structures, the records contained within a VDE card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements. '193 patent 41:37-42.

	Claim Term / Phrase	InterTrust Evidence
		19(E) SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected. '193 patent 59:48-59. **19(F)** VDE 100 stores separately deliverable VDE elements in a secure (e.g., encrypted) database 610 distributed to each VDE electronic appliance 610. '193 patent 126:6-8. **19(G)** Secure (tamper-resistant) executable code. '193 patent 126:30-31. **19(H)** In one embodiment, the portable appliance 2600 could support secure (in this instance encrypted and/or authenticated) two-way communications with a retail terminal which may contain a VDE electronic appliance 600 or communicate with a retailer's or third party provider's VDE electronic appliance 600. '193 patent 233:25-30.

	Claim Term / Phrase	InterTrust Evidence
		19(I) Information could then be automatically "parsed" and routed into securely maintained (for example, encrypted) appropriate database management records within portable appliance 2600. '193 patent 233:51-54. **19(J)** The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely. '193 patent at 49:59-62. **19(K)** There are many ways in which a PPE 650 might be compromised. The goal of the security provided by VDE 100 is to reduce the possibility that the system will be compromised, and minimize the adverse effects if it is compromised. '193 patent at 221:2-6. **19(L)** VDE 100 provided by the preferred embodiment has sufficient security to help ensure that it cannot be compromised short of a successful "brute force attack," and so that the time and cost to succeed in such a "brute force attack" substantially exceeds any value to be derived. In addition, the security provided by VDE 100 compartmentalizes the internal workings of VDE so that a successful "brute force attack" would compromise only a strictly bounded subset of protected information, not the entire system. '193 patent at 199:38-46. **19(M)** VDE supports trusted (sufficiently secure) electronic information

	Claim Term / Phrase	InterTrust Evidence
		distribution and usage control models for both commercial electronic content distribution and data security applications. '193 patent at 16:25-28.
		19(N) Because security may be better/more effectively enforced with the assistance of hardware security features such as those provided by SPU 500 (and because of other factors such as increased performance provided by special purpose circuitry within SPU 500), at least one SPE 503 is preferred for many or most higher security applications. However, in applications where lesser security can be tolerated and/or the cost of an SPU 500 cannot be tolerated, the SPE 503 may be omitted and all secure processing may instead be performed by one or more secure HPEs 655 executing on general-purpose CPUs 654. '193 patent at 80:65-81:8.
		19(O) 1. A security method comprising: (a) digitally signing a first load module with a first digital signature designating the first load module for use by a first device class; (b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class; (c) distributing the first load module for use by at least one device in the first device class; and (d) distributing the second load module for use by at least one device in the second device class. '721 patent at 21:9-24.

	Claim Term / Phrase	InterTrust Evidence
		19(P) 34. A protected processing environment comprising: a first tamper resistant barrier having a first security level, a first secure execution space, and at least one arrangement within the first tamper resistant barrier that prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level. '721 patent at 24:48-56. **19(Q)** [VDE features] support security techniques that materially increase the time required to "break" a system's integrity. This includes using a collection of techniques that minimizes the damage resulting from comprising some aspect of the security features of the present inventions. '193 patent at 35:59-63. **19(R)** Fingerprinting electronic content before it is encrypted for transfer to a customer or other user provides information that can be very useful for identifying who received certain content which may have then been distributed or made available in unencrypted form. This information would be useful in tracking who may have "broken" the security of a VDE installation and was illegally making certain electronic content available to others. '193 patent at 38:4-12. **19(S)** If a content key becomes compromised, the portion of the content encrypted with the key is also compromised until the key "ages" and

	Claim Term / Phrase	InterTrust Evidence
		expires. If the "aging" process for that key also becomes compromised, then the breach becomes permanent. '193 patent at 222:49-53. --- **19(T)** If PPE 650 (or a VDE administrator watching its activities or communicating with it) detects that it has been compromised, it may be updated with an initialization to use new code, keys and new encryption/decryption algorithms. This would limit exposure to VDE objects 300 that existed at the time the encryption scheme was broken. '193 patent at 223:4-10. --- **Extrinsic Sources** **19(U)** **security** The protection of valuable assets stored on computer systems or transmitted via computer networks. Computer security involves the following conceptually differentiated areas: • **Authentication** (ensuring that users are indeed the persons they claim to be). • **Access control** (ensuring that users access only those resources and services that they are entitled to access). • **Confidentiality** (ensuring that transmitted or stored data is not examined by unauthorized persons). • **Integrity** (ensuring that transmitted or stored data is not altered by unauthorized persons in a way that is not detectable by authorized users). • **Nonrepudiation** (ensuring that qualified users are not denied access to services that they legitimately expect to receive, and that originators of messages cannot deny that they in fact sent a given message). Webster's New World Dictionary of Computer Terms, 6th ed. (1997), p. 463. ---

	Claim Term / Phrase	InterTrust Evidence
		Citations from Sources Designated by Microsoft under PLR 4-2(b) **19(V)** In common technical usage, however, computer security and communication security generally refer to protection against human misuse, and exclude the protection against malfunctions. Neumann, Computer Related Risks (ACM Press, 1995), p. 96. **19(W)** There is a fifth important attribute of dependability—the *security attribute*—that cannot be measured easily: the ability of a system to prevent unauthorized access or handling of information. Mullender, Distributed Systems, 2nd ed. (Addison-Wesley, 1993), p. 420. **19(X)** Furthermore, there is never an absolute sense in which a system is secure or reliable. Neumann, Computer Related Risks (ACM Press, 1995), p. 2. **19(Y)** The fundamental purpose of security is to minimize the risk of loss from (1) physical damage or destruction, (2) human errors and omissions, and (3) theft or unauthorized disclosure. That purpose is best fulfilled by effective loss-prevention efforts. Loss-prevention efforts involve the identification and assessment of risks to capital, human, informational, and technological assets, and the development of suitable and cost-feasible countermeasures. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 75. **19(Z)** Total software security is no more attainable than is perfect security in any other area. A highly skilled programmer can almost

	Claim Term / Phrase	InterTrust Evidence
		always penetrate software safeguards written by another programmer. Of course, the same can be said for attorneys; an unprincipled lawyer can usually get around protections in a contract written by an-other lawyer. Yet contracts continue to be written, and, for the most part, they are effective. Computer software security routines can also be effective most of the time. A security procedure does not have to be all-encompassing; if it provides reasonable protection at an acceptable cost, it is certainly worthwhile. The basic consideration is one of degree—how important are specific elements of data and software, and how important is their security. Some data require very little security. For example, a software library containing programs that are similar to those found in many other computer installations does not require elaborate security protection against theft. On the other hand, proprietary programs and sensitive data require extensive security. A data base containing payroll information requires stringent security procedures to maintain its confidentiality. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 201. **19(AA)** Regardless of which form of data storage is being considered, one must bear in mind a vital concept: no data processing installation can afford 100 percent security—if indeed there is such a thing. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 218. **19(BB)** One hundred percent security cannot be achieved. The most effective systems apply security protection techniques in layers. Each layer of protection diminishes the chances of someone breaking through the barriers. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), pp. 293. **19(CC)** Risk analysis is not intended to come up with a plan for absolute security. Indeed, absolute security is not achievable in today's

	Claim Term / Phrase	InterTrust Evidence
		computer systems. Rather, risk analysis produces a degree of security commensurate with the information to be protected and with the amount of resources to be expended. Hoffman, Modern Methods for Computer Security and Privacy (Prentice-Hall, 1977), p. 170. **19(DD)** No matter how secure you make them, computers can always be broken into given sufficient resources, time, and money. Computers are especially vulnerable because software is complex and we don't always know if there are flaws present that make the task of breaking in easier. Even systems that are certified according to the Department of Defense's so-called Orange Book are vulnerable, especially if they are not administered correctly. Just as six-foot-thick vaults doors don't work if they're not administered properly. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), pp. 13. **19(EE)** Security is a relative, not an absolute, concept, and gains in security often come only with penalties in performance. Landwehr, Formal Models for Computer Security, ACM Computer Surveys (Sept. 3, 1981), p. 253.

	Claim Term / Phrase	InterTrust Evidence
20.	**secure container** 912.35, 861.58, 683.2	**Patent Specifications** **20(A)** The "container" concept is a convenient metaphor used to give a name to the collection of elements required to make use of content or to perform an administrative-type activity. Container 302 typically includes identifying information, control structures and content (e.g., a property or administrative data). The term "container" is often (e.g., Bento/OpenDoc and OLE) used to describe a collection of information stored on a computer system's secondary storage system(s) or accessible to a computer system over a communications network on a "server's" secondary storage system. The "container" 302 provided by the preferred embodiment is not so limited or restricted. In VDE 100, there is no requirement that this information is stored together, received at the same time, updated at the same time, used for only a single object, or be owned by the same entity. Rather, in VDE 100 the container concept is extended and generalized to include real-time content and/or online interactive content passed to an electronic appliance over a cable, by broadcast, or communicated by other electronic communication means. '193 patent 127:30-49. --- **20(B)** VDE, in its preferred embodiment, employs object software technology and uses object technology to form "containers" for delivery of information that is (at least in part) encrypted or otherwise secured. These containers may contain electronic content products or other electronic information and some or all of their associated permissions (control) information. These container objects may be distributed along pathways involving content providers and/or content users. They may be securely moved among nodes of a Virtual Distribution Environment (VDE) arrangement, which nodes operate VDE foundation software and execute control methods to enact electronic information usage control and/or administration models. The containers delivered through use of the preferred embodiment of the present invention may be employed both for distributing VDE control instructions (information) and/or to encapsulate and electronically distribute content that has been at least partially secured. '193 patent 13:54-14:4.

	Claim Term / Phrase	InterTrust Evidence
		20(C) Figure 88 illustrates secure electronic container 302 as an attaché case handcuffed to the secure delivery person's wrist. Once again, container is shown as a physical thing for purposes of illustration only -- in the example it is preferably electronic rather than physical, and comprises digital information having a well-defined structure (see Figure 5A). Special mathematical techniques known as "cryptography" can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other item) 4054 it contains. '683 patent 15:61-16:4. --- **20(D)** The Figure 5A example shows items "within" and enclosed by container 302. However, container 302 may "contain" items without those items actually being stored within the container. For example, the container 302 may reference items that are available elsewhere such as in other containers at remote sites. Container 302 may reference items available at different times or only during limited times. Some items may be too large to store within container 302. Items may, for example, be delivered to the user in the form of a "live feed" of video at a certain time. Even then, the container 302 "contains" the live feed (by reference) in this example. '193 patent 58:48-58. --- **20(E)** The term "container" is often (e.g., Bento/OpenDoc and OLE) used to describe a collection of information stored on a computer system's secondary storage system(s) or accessible to a computer system over a communications network on a "server's" secondary storage system. The "container" 302 provided by the preferred embodiment is not so limited or restricted. In VDE 100, there is no requirement that this information is stored together, received at the same time, updated at the same time, used for only a single object, or be owned by the same entity. Rather, in VDE 100 the container concept is extended and generalized to include real-time content and/or online interactive content passed to an electronic appliance

	Claim Term / Phrase	InterTrust Evidence
		over a cable, by broadcast, or communicated by other electronic communication means. Thus, the "complete" VDE container 302 or logical object structure 800 may not exist at the user's location (or any other location, for that matter) at any one time. The "logical object" may exist over a particular period of time (or periods of time), rather than all at once. This concept includes the notion of a "virtual container" where important container elements may exist either as a plurality of locations and/or over a sequence of time periods (which may or may not overlap). Of course, VDE 100 containers can also be stored with all required control structures and content together. This represents a continuum: from all content and control structures present in a single container, to no locally accessible content or container specific control structures. '193 patent 127:35-62. **20(F)** In order to improve performance, the containers themselves may remain at the users' sites, and only the encrypted contents transmitted between the participants. '683 patent 53:3-5. **20(G)** In more detail, the logical object structure 800 provided by the preferred embodiment includes a public (or unencrypted) header 802 that identifies the object and may also identify one or more owners of rights in the object and/or one or more distributors of the object. Private (or encrypted) header 804 may include a part or all of the information in the public header and further, in the preferred embodiment, will include additional data for validating and identifying the object 300 when a user attempts to register as a user of the object with a service clearinghouse, VDE administrator, or an SPU 500. Alternatively, information identifying.... '193 patent 128:11-21.

	Claim Term / Phrase	InterTrust Evidence
		20(H) Third party go-between can authenticate an item by, for example, opening (e.g. decrypting content) one or more containers '683 patent 9:59-61. --- **Extrinsic Sources** **20(I)** **container** *n.* **1.** In OLE terminology, a file containing linked or embedded objects. *See also* OLE. **2.** In SGML, an element that has content as opposed to one consisting solely of the tag name and attributes. Microsoft Computer Dictionary, 3d, ed. (Microsoft Press, 1997), p. 115. --- **20(J)** In a preferred embodiment of the present invention, an application program that creates a compound document controls the manipulation of linked or embedded data generated by another application. In object-oriented parlance, this data is referred to as an object. (The reference Budd, T., "An Introduction to Object-Oriented Programming," Addison-Wesley Publishing Co., Inc., 1991, provides an introduction to object-oriented concepts and terminology.) An object that is either linked or embedded into a compound document is "contained" within the document. Also, a compound document is referred to as a "container" object and the objects contained within a compound document are referred to as "contained" or "containee" objects. Referring to FIGS. 1 and 2, the scheduling data 102 and budgeting data 103 are containee objects and the compound document 101 is a container object. USP 5,634,019 at 7:34-49.

	Claim Term / Phrase	InterTrust Evidence
21.	**tamper resistance** 721.1	**Patent Specifications** **21(A)** Maintaining shared secrets (e.g., cryptographic keys) within a tamper resistant enclosure that the owner of the electronic appliance cannot easily tamper with. '721 patent at 4:40-42. --- **21(B)** SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected. '193 patent at 59:48-59. --- **Extrinsic Sources** **21(C)** To evaluate the results of physically protecting portions of the system, the concept of a tamper-resistant module (TRM) is introduced. All information contained within a TRM is protected from disclosure and undetected modification in the following sense. As long as the TRM is intact, data inside the module cannot be discerned or modified by an attacker and if the TRM is breached the sensitive data within is destroyed (erased). The implementation of TRMs will vary considerably depending on the value of the external software being protected and the perceived sophistication of potential attackers. Kent, Protecting Externally Supplied Software in Small Computers, Doctoral Thesis (Sept. 22, 1980), p. PA00000363.

	Claim Term / Phrase	InterTrust Evidence
		21(D) Tamper-resistant software is software which is resistant to observation and modification. It can be trusted/ within certain bounds/ to operate as intended even in the presence of a malicious attack. Our approach has been to classify attacks into three categories and then to develop a series of software design principles that allow a scaled response to those threats. Aucsmith, Tamper Resistant Software: An Implementation (1996), p. PA00002323. **21(E)** Tamper-resistance ensures proper operation of a program and prevents extraction of secret data and abuse of the program. Moreover tamper-resistance enables a vendor to enforce his own conditions upon users. Mambo et al., A Tentative Approach to Constructing Tamper-Resistant Software, School of Information Science, Japan Advanced Institute of Science and Technology, 1-1 Asahidai Tatsunokuchi Nomi, Ishikawa (1997), p. PA00005363.

	Claim Term / Phrase	InterTrust Evidence
22.	**tamper resistant barrier** 721.34	**Patent Specifications** **22(A)** SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected. '193 patent 59:48-59. **22(B)** HPEs 655 may (as shown in Figure 10) be provided with a software-based tamper resistant barrier 674 that makes them more secure. Such a software-based tamper resistant barrier 674 may be created by software executing on general-purpose CPU 654. Such a "secure" HPE 655 can be used by ROS 602 to execute processes that, while still needing security, may not require the degree of security provided by SPU 500. This can be especially beneficial in architectures providing both an SPE 503 and an HPE 655. The SPU 502 may be used to perform all truly secure processing, whereas one or more HPEs 655 may be used to provide additional secure (albeit possibly less secure than the SPE) processing using host processor or other general purpose resources that may be available within an electronic appliance 600. Any service may be provided by such a secure HPE 655. In the preferred embodiment, certain aspects of "channel processing" appears to be a candidate that could be readily exported from SPE 503 to HPE 655. The software-based tamper resistant barrier 674 provided by HPE 655 may be provided, for example, by: introducing time checks and/or code modifications to complicate the process of stepping through code comprising a portion of kernel 688a and/or a portion of component assemblies 690 using a debugger; using a map of defects on a storage device (e.g., a hard disk, memory card, etc.) to form internal test values to impede moving and/or copying HPE 655 to other electronic appliances 600; using kernel code that contains

	Claim Term / Phrase	InterTrust Evidence
		false branches and other complications in flow of control to disguise internal processes to some degree from disassembly or other efforts to discover details of processes; using "self-generating" code (based on the output of a co-sine transform, for example) such that detailed and/or complete instruction sequences are not stored explicitly on storage devices and/or in active memory but rather are generated as needed; using code that "shuffles" memory locations used for data values based on operational parameters to complicate efforts to manipulate such values; using any software and/or hardware memory management resources of electronic appliance 600 to "protect" the operation of HPE 655 from other processes, functions, etc. Although such a software-based tamper resistant barrier 674 may provide a fair degree of security, it typically will not be as secure as the hardware-based tamper resistant barrier 502 provided (at least in part) by SPU 500. '193 patent 80:22-65. **22(C)** Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. Tamper resistant barriers may be used to protect this programming or other conditioning. '721 patent 5:1-6.

	Claim Term / Phrase	InterTrust Evidence
23.	use 912.8, 912.35, 861.58, 193.19, 891.1, 683.2, 721.1	**Extrinsic Sources** 23(A) **use** *v.* **used, us-ing, us-es.** *tr.* **1.** To put into service or apply for a purpose; employ. **2.** To avail oneself of; practice: *use caution.* **3.** To conduct oneself toward; treat or handle: *"the peace offering of a man who once used you unkindly"* (Laurence Sterne). **4.** To seek or achieve an end by means of; exploit: *used their highly placed friends to gain access to the president; felt he was being used by seekers of favor.* **5.** To take or consume; partake of: *She rarely used alcohol.* –intr. (yoos, yoost). Used in the past tense followed by *to* in order to indicate a former state, habitual practice, or custom: *Mail service used to be faster.* **use** (yoos). *n.* **1. a.** The act of using; the application or employment of something for a purpose: *with the use of a calculator; skilled in the use of the bow and arrow.* **b.** The condition or fact of being used: *a chair in regular use.* **2.** The manner of using; usage: *learned the proper use of power tools.* **3. a.** The permission, privilege, or benefit of using something: *gave us the use of their summerhouse.* **b.** The power or ability to use something: *lost the use of one arm.* **4.** The need or occasion to use or employ: *have no use for these old clothes.* **5.** The quality of being suitable or adaptable to an end; usefulness: *tried to be of use in the kitchen.* **6.** A purpose for which something is used: *a tool with several uses; a pretty bowl, but of what use is it?* **7.** Gain or advantage; good: *There's no use in discussing it. What's the use?* **8.** Accustomed or usual procedure or practice. **9.** *Law.* **a.** Enjoyment of property, as by occupying or exercising it. **b.** The benefit or profit of lands and tenements of which the legal title and possession are vested in another. **c.** The arrangement establishing the equitable right to such benefits and profits. **10.** A liturgical form practiced in a particular church, ecclesiastical district, or community. **11.** *Obsolete.* Usual occurrence or experience. **--phrasal verb. use up.** To consume completely: *used up all our money.* [Middle English *usen*, from Old French *user*, from Vulgar Latin **usare*, frequentative of Latin *uti.*] ***SYNONYM:*** *use, employ, utilize.* These verbs mean to avail oneself of someone or something in order to make him, her, or it useful, functional, or beneficial. To *use* is to put into service or apply for a purpose: *uses a hearing aid; used the press secretary as spokesperson for the administration; using a stick to stir the paint. Employ* is often interchangeable with *use*: *She employed her education to maximum advantage.* Unlike *use*, however, the term can denote engaging or maintaining the services of another or putting another to work: *"When men are employed, they are best*

	Claim Term / Phrase	InterTrust Evidence
		contented" (Benjamin Franklin). *Utilize* is especially appropriate in the narrower sense of making something profitable or of finding new and practical uses for it: *In the 19th century waterpower was widely utilized to generate electricity.* See also Synonyms at **habit.** American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1966.

	Claim Term / Phrase	InterTrust Evidence
24.	virtual distribution environment 900.155	**Patent Specifications** **24(A)** VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information. '193 patent at 9:36-39; '900 patent at 9:33-36. **24(B)** Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Secure subsystems used with such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. '900 patent at Abstract. **24(C)** Figure 1 shows a "Virtual Distribution Environment" ("VDE") 100 that may be provided in accordance with this invention. In Figure 1, an information utility 200 connects to communications means 202 such as telephone or cable TV lines for example. Telephone or cable TV lines 202 may be part of an "electronic highway" that carries electronic information from place to place. Lines 202 connect information utility 200 to other people such as for example a consumer 208, an office 210, a video production studio 204, and a publishing house 214. Each of the people connected to information utility 200 may be called a "VDE participant" because they can participate in transactions occurring within the virtual distribution environment 100. Almost any sort of transaction you can think of can be supported by virtual distribution environment 100. A few of many examples of

	Claim Term / Phrase	InterTrust Evidence
		transactions that can be supported by virtual distribution environment 100 include: home banking and electronic payments; electronic legal contracts; distribution of "content" such as electronic printed matter, video, audio, images and computer programs; and secure communication of private information such as medical records and financial information. Virtual distribution environment 100 is "virtual" because it does not require many of the physical "things" that used to be necessary to protect rights, ensure reliable and predictable distribution, and ensure proper compensation to content creators and distributors. For example, in the past, information was distributed on records or disks that were difficult to copy. In the past, private or secret content was distributed in sealed envelopes or locked briefcases delivered by courier. To ensure appropriate compensation, consumers received goods and services only after they handed cash over to a seller. Although information utility 200 may deliver information by transferring physical "things" such as electronic storage media, the virtual distribution environment 100 facilitates a completely electronic "chain of handling and control." '193 patent at 52:66-53:37; '900 patent 53:39-54:10.
		24(D) Because security may be better/more effectively enforced with the assistance of hardware security features such as those provided by SPU 500 (and because of other factors such as increased performance provided by special purpose circuitry within SPU 500), at least one SPE 503 is preferred for many or most higher security applications. However, in applications where lesser security can be tolerated and/or the cost of an SPU 500 cannot be tolerated, the SPE 503 may be omitted and all secure processing may instead be performed by one or more secure HPEs 655 executing on general-purpose CPUs 654. '193 patent 80:65-67-81:8.

	Claim Term / Phrase	InterTrust Evidence
		24(E) An end user may make use of credit and/or currency securely stored within the end user's VDE installation secure subsystem to pay for charges related to use of VDE content received from the repository, and/or the user may maintain a secure credit and/or currency account remotely at the repository, including a "virtual" repository where payment is made for the receipt of such content by an end user. This later approach may provide greater assurance for payment to the repository and/or content providers particularly if the end user has only an HPE based secure subsystem. '193 patent at 291:39-49; '900 patent 316:35-45. **24(F)** Large Organization Example In a somewhat more general example, suppose an organization (e.g., a corporation or government department) with thousands of employees and numerous offices disposed throughout a large geographic area wishes to exercise control over distribution of information which belongs to said organization (or association). '193 patent at 277:26-32; '900 patent 302:17-24. **24(G)** User Environment In an organization (or association) such as that described above, users may utilize a variety of electronic appliances 600 for processing and managing documents. This may include personal computers, both networked and otherwise, powerful single-user workstations, and servers or mainframe computers. To provide support for the control information described in this example, each electronic appliance that participates in use and management of VDE-protected documents may be enhanced with a VDE secure subsystem supporting an SPE, S03 and/or HPE 655. In some organizations, where the threats to secure operation are relatively low, an HPE 655 may suffice. In other organizations (e.g., government defense), it may be necessary to employ an SPE

	Claim Term / Phrase	InterTrust Evidence
		503 in all situations where VDE-protected documents are processed. The choice of enhancement environment and technology may be different in different of the organization. Even if different types of PPE 650 are used within an organization to serve different requirements, they may be compatible and may operate on the same types (or subsets of types) of documents. '193 patent at 278:45-65; '900 patent 303:40-61.
		24(H) HPEs 655 may (as shown in Figure 10) be provided with a software-based tamper resistant barrier 674 that makes them more secure. Such a software-based tamper resistant barrier 674 may be created by software executing on general-purpose CPU 654. Such a "secure" HPE 655 can be used by ROS 602 to execute processes that, while still needing security, may not require the degree of security provided by SPU 500. This can be especially beneficial in architectures providing both an SPE 503 and an HPE 655. The SPU 502 may be used to perform all truly secure processing, whereas one or more HPEs 655 may be used to provide additional secure (albeit possibly less secure than the SPE) processing using host processor or other general purpose resources that may be available within an electronic appliance 600. Any service may be provided by such a secure HPE 655. In the preferred embodiment, certain aspects of "channel processing" appears to be a candidate that could be readily exported from SPE 503 to HPE 655. The software-based tamper resistant barrier 674 provided by HPE 655 may be provided, for example, by: introducing time checks and/or code modifications to complicate the process of stepping through code comprising a portion of kernel 688a and/or a portion of component assemblies 690 using a debugger; using a map of defects on a storage device (e.g., a hard disk, memory card, etc.) to form internal test values to impede moving and/or copying HPE 655 to other electronic appliances 600; using kernel code that contains false branches and other complications in flow of control to disguise internal processes to some degree from disassembly or other efforts to discover details of processes; using "self-generating" code (based on the output of a co-sine transform, for example) such that detailed and/or complete instruction sequences are not stored explicitly on storage devices and/or in active memory but rather are generated as needed; using code that "shuffles" memory locations used for data values based on operational parameters to complicate efforts to manipulate such values; using any software and/or hardware

	Claim Term / Phrase	InterTrust Evidence
		memory management resources of electronic appliance 600 to "protect" the operation of HPE 655 from other processes, functions, etc. Although such a software-based tamper resistant barrier 674 may provide a fair degree of security, it typically will not be as secure as the hardware-based tamper resistant barrier 502 provided (at least in part) by SPU 500. '193 patent 80:22-65. **24(I)** VDE supplies an efficient, largely transparent, low cost and sufficiently secure system (supporting both hardware/ software and software only models). '193 patent at 9:11-13; '900 patent 9:8-10. **24(J)** 10. A method as in claim 1 in which said steps of receiving, providing, performing and producing occur within a Virtual Distribution Environment. 11. A system as in claim 2 in which said first location and said second location are contained within a Virtual Distribution Environment. 12. A system as in claim 3 in which said first location and said second location are contained within a Virtual Distribution Environment. 13. A system as in claim 6 in which said protected processing environment is contained within a Virtual Distribution Environment. 14. A method as in claim 9 in which said first location and said second location are contained within a Virtual Distribution Environment. USP 5,949,876 at 320:14-28.

	Claim Term / Phrase	InterTrust Evidence
		24(K) The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely. '193 patent at 49:59-62. **24(L)** There are many ways in which a PPE 650 might be compromised. The goal of the security provided by VDE 100 is to reduce the possibility that the system will be compromised, and minimize the adverse effects if it is compromised. '193 patent at 221:2-6. **24(M)** VDE 100 provided by the preferred embodiment has sufficient security to help ensure that it cannot be compromised short of a successful "brute force attack," and so that the time and cost to succeed in such a "brute force attack" substantially exceeds any value to be derived. In addition, the security provided by VDE 100 compartmentalizes the internal workings of VDE so that a successful "brute force attack" would compromise only a strictly bounded subset of protected information, not the entire system. '193 patent at 199:38-46. **24(N)** VDE supports trusted (sufficiently secure) electronic information distribution and usage control models for both commercial electronic content distribution and data security applications. '193 patent at 16:25-28. **24(O)** Employing VDE as a general purpose electronic

	Claim Term / Phrase	InterTrust Evidence
		transaction/distribution control system allows users to maintain a single transaction management control arrangement on each of their computers, networks, communication nodes, and/or other electronic appliances. Such a general purpose system can serve the needs of many electronic transaction management applications without requiring distinct, different installations for different purposes. As a result, users of VDE can avoid the confusion and expense and other inefficiencies of different, limited purpose transaction control applications for each different content and/or business model. '193 patent at 11:38-49; '900 patent at 11:36-47. **24(P)** [VDE features] support security techniques that materially increase the time required to "break" a system's integrity. This includes using a collection of techniques that minimizes the damage resulting from comprising some aspect of the security features of the present inventions. '193 patent at 35:59-63 **24(Q)** Fingerprinting electronic content before it is encrypted for transfer to a customer or other user provides information that can be very useful for identifying who received certain content which may have then been distributed or made available in unencrypted form. This information would be useful in tracking who may have "broken" the security of a VDE installation and was illegally making certain electronic content available to others. '193 patent at 38:4-12 **24(R)** If a content key becomes compromised, the portion of the content encrypted with the key is also compromised until the key "ages" and expires. If the "aging" process for that key also becomes compromised, then the breach becomes permanent. '193 patent at 222:49-53.

	Claim Term / Phrase	InterTrust Evidence
		24(S) If PPE 650 (or a VDE administrator watching its activities or communicating with it) detects that it has been compromised, it may be updated with an initialization to use new code, keys and new encryption/decryption algorithms. This would limit exposure to VDE objects 300 that existed at the time the encryption scheme was broken. '193 patent at 223:4-10. --- **Citations from Sources Designated by Microsoft under PLR 4-2(b)** **24(T)** Furthermore, there is never an absolute sense in which a system is secure or reliable. Neumann, Computer Related Risks (ACM Press, 1995), p. 2. --- **24(U)** The fundamental purpose of security is to minimize the risk of loss from (1) physical damage or destruction, (2) human errors and omissions, and (3) theft or unauthorized disclosure. That purpose is best fulfilled by effective loss-prevention efforts. Loss-prevention efforts involve the identification and assessment of risks to capital, human, informational, and technological assets, and the development of suitable and cost-feasible countermeasures. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 75. --- **24(V)** Total software security is no more attainable than is perfect security in any other area. A highly skilled programmer can almost always penetrate software safeguards written by another programmer. Of course, the same can be said for attorneys; an unprincipled lawyer can usually get around protections in a contract written by an-other lawyer. Yet contracts continue to be written, and, for the most part, they are effective. Computer software security routines can also be effective most of the time. A

	Claim Term / Phrase	InterTrust Evidence
		security procedure does not have to be all-encompassing; if it provides reasonable protection at an acceptable cost, it is certainly worthwhile. The basic consideration is one of degree—how important are specific elements of data and software, and how important is their security. Some data require very little security. For example, a software library containing programs that are similar to those found in many other computer installations does not require elaborate security protection against theft. On the other hand, proprietary programs and sensitive data require extensive security. A data base containing payroll information requires stringent security procedures to maintain its confidentiality. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 201. **24(W)** Regardless of which form of data storage is being considered, one must bear in mind a vital concept: no data processing installation can afford 100 percent security—if indeed there is such a thing. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 218. **24(X)** One hundred percent security cannot be achieved. The most effective systems apply security protection techniques in layers. Each layer of protection diminishes the chances of someone breaking through the barriers. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), pp. 293. **24(Y)** Risk analysis is not intended to come up with a plan for absolute security. Indeed, absolute security is not achievable in today's computer systems. Rather, risk analysis produces a degree of security commensurate with the information to be protected and with the amount of resources to be expended. Hoffman, Modern Methods for Computer Security and Privacy (Prentice-Hall, 1977), p. 170.

	Claim Term / Phrase	InterTrust Evidence
		24(Z) No matter how secure you make them, computers can always be broken into given sufficient resources, time, and money. Computers are especially vulnerable because software is complex and we don't always know if there are flaws present that make the task of breaking in easier. Even systems that are certified according to the Department of Defense's so-called Orange Book are vulnerable, especially if they are not administered correctly. Just as six-foot-thick vaults doors don't work if they're not administered properly. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), pp. 13. **24(AA)** Security is a relative, not an absolute, concept, and gains in security often come only with penalties in performance. Landwehr, Formal Models for Computer Security, ACM Computer Surveys (Sept. 3, 1981), p. 253. **File Histories** **24(BB)** 1. Restriction to one of the following inventions is required under 35 U.S.C. § 121: Group I . . . drawn to a secure component-based operating process, classified in Classs 380, subclass 25. Group II. . . . drawn to method(s) for managing a resource or operating, classified in Class 380, subclass 4. Group III. . . . drawn to a secure method, classified in Class 380, subclass 3. Group IV. . . . drawn to [a] method of negotiating electronic contracts, classified in Class 364, subclass 401. Group V. . . . drawn to methods of auditing a resource, classified in Class 364, subclass 406.

	Claim Term / Phrase	InterTrust Evidence
		The inventions are distinct, each from the other because of the following reasons: 2. Inventions of Groups I-V are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention of Group I has separate utility such as protecting executable code from computer viruses. Invention of Group II has separate utility such as a computer network administration. Invention of Group III has separate utility such as protection of software. Invention of Group IV has separate utility such as a contract bidding procedure. Invention of Group V has separate utility such as auditing pay television. . . . 3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper. 4. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper. '193 File History, 9/25/96 Office Action, pp. 2-3 (a complete copy of this document is attached to the Declaration of Douglas K. Derwin In Support of InterTrust's Claim Construction Position).

	Claim Term / Phrase	InterTrust Evidence
25.	193.1: "a budget specifying the number of copies which can be made of said digital file"	**Patent Specifications** **25(A)** Traveling objects can also be used to facilitate "moving" an object from one electronic appliance 600 to another. A user could move a traveling object, with its incorporated one or more permission records 808 from a desktop computer, for example, to his notebook computer. A traveling object might register its user within itself and thereafter only be useable by that one user. A traveling object might maintain separate budget information, one for the basic distribution budget record, and another for the "active" distribution budget record of the registered user. In this way, the object could be copied and passed to another potential user, and then could be a portable object for that user. '193 patent at 133:39-50. **25(B)** Meters and budgets are perhaps among the most common data structures in VDE 100. They are used to count and record events, and also to limit events. The data structures for each meter and budget are determined by the content provider or a distributor/redistributor authorized to change the information. Meters and budgets, however, generally have common information stored in a common header format (e.g., user ID, site ID and related identification information). The content provider or distributor/redistributor may specify data structures for each meter and budget UDE. Although these data structures vary depending upon the particular application, some are more common than others. The following table lists some of the more commonly occurring data structures for METER and BUDGET methods: Field type / Format / Typical Use / Description or Use Ascending Use Counter / byte, short, long, or unsigned versions of the / Meter /Budget / Ascending count of uses.

	Claim Term / Phrase	InterTrust Evidence

	same widths	
Descending Use Counter	byte, short, long, or unsigned versions of the same widths	Budget	Descending count of permitted use, eg., remaining budget.
Counter /Limit	2, 4 or 8 byte integer split into two related bytes or words	Meter /Budget	usage limits since a specific time, generally used in compound meter data structures.
Bitmap	Array bytes	Meter /Budget	Bit indicator of use or ownership.
Wide bitmap	Array of bytes	Meter /Budget	Indicator of use or ownership that may age with time.
Last Use Date	time_t	Meter /Budget	Date of last use.
Start Date	time_t	Budget	Date of first allowable use.
Expiration Date	time_t	Meter /Budget	Expiration Date.
Last Audit Date	time_t	Meter /Budget	Date of last audit.
Next Audit Date	time_t	Meter /Budget	Date of next required audit.
Auditor	VDE ID	Meter /Budget	VDE ID of authorized auditor.

The information in the table above is not complete or comprehensive, but rather is intended to show some examples of types of information that may be stored in meter and budget related data structures. The actual structure of particular meters and budgets is determined by one or more DTDs 1108 associated with

	Claim Term / Phrase	InterTrust Evidence
		the load modules 1100 that create and manipulate the data structure. A list of data types permitted by the DTD interpreter 590 in VDE 100 is extensible by properly authorized parties. '193 patent at 143:38-144:31. --- **25(C)** During the same or different communications exchange, the same or different clearinghouse may handle the end user's request for additional budget and/or permission pertaining to VDE object 300. For example, the end user's electronic appliance 600 may (e.g., in response to a user input request to access a particular VDE object 300) send an administrative object to the clearinghouse requesting budgets and/or other permissions allowing access (Block 1164). As mentioned above, such requests may be transmitted in the form of one or more administrative objects, such as, for example, a single administrative object having multiple "events" associated with multiple requested budgets and/or other permissions for the same or different VDE objects 300. The clearinghouse may upon receipt of such a request, check the end user's credit, financial records, business agreements and/or audit histories to determine whether the requested budgets and/or permissions should be given. The clearinghouse may, based on this analysis, send one or more responsive administrative objects which cause the end user's electronic appliance 600 to update its secure database in response (Block 1166, 1168). This updating might, for example, comprise replacing an expired PERC 808 with a fresh one, modifying a PERC to provide additional (or lesser) rights, etc. Steps 1164-1168 may be repeated multiple times in the same or different communications session to provide further updates to the end user's secure database 610. '193 patent at 162:39-65. --- **25(D)** In the example shown in Figure 41d, a distributor at a VDE distributor node (106) might request budget from a content creator at another node (102). This request may be made in the context of a secure VDE communication or it may be passed in an "out-of-channel" communication (e.g. a telephone call or letter). The creator 102 may decide to grant budget to the distributor 106 and

	Claim Term / Phrase	InterTrust Evidence
		processes a distribute event (1452 in BUDGET method 1510 at VDE node 102). A result of processing the distribute event within the BUDGET method might be a secure communication (1454) between VDE nodes 102 and 106 by which a budget granting use and redistribute rights to the distributor 106 may be transferred from the creator 102 to the distributor. The distributor's VDE node 106 may respond to the receipt of the budget information by processing the communication using the reply process 1475B of the BUDGET method 1510. The reply event processing 1475B might, for example, install a budget and PERC 808 within the distributor's VDE 106 node to permit the distributor to access content or processes for which access is control at least in part by the budget and/or PERC. At some point, the distributor 106 may also desire to use the content to which she has been granted rights to access. After registering to use the content object, the user 112 would be required to utilize an array of "use" processes 1476C to, for example, open, read, write, and/or close the content object as part of the use process. Once the distributor 106 has used some or all of her budget, she may desire to obtain additional budget. The distributor 106 might then initiate a process using the BUDGET method request process (1480B). Request process 1480B might initiate a communication (1482AB) with the content creator VDE node 102 requesting more budget and perhaps providing details of the use activity to date (e.g., audit trails). The content creator 102 processes the 'get more budget' request event 1482AB using the response process (1484A) within the creator's BUDGET method 1510A. Response process 1484A might, for example, make a determination if the use information indicates proper use of the content, and/or if the distributor is credit worthy for more budget. The BUDGET method response process 1484A might also initiate a financial transaction to transfer funds from the distributor to pay for said use, or use the distribute process 1472A to distribute budget to the distributor 106. A response to the distributor 106 granting more budget (or denying more budget) might be sent immediately as a response to the request communication 1482AB, or it might be sent at a later time as part of a separate communication. The response communication, upon being received at the distributor's VDE node 106, might be processed using the reply process 1475B within the distributor's copy of the BUDGET method 1510B. The reply process 1475B might then process the additional budget in the same manner as described above. The chain of handling and control may, in addition to posting

	Claim Term / Phrase	InterTrust Evidence
		budget information, also pass control information that governs the manner in which said budget may be utilized. For example, the control information specified in the above example may also contain control information describing the process and limits that apply to the distributor's redistribution of the right to use the creator's content object. Thus, when the distributor responds to a budget request from a user (a communication between a user at VDE node 112 to the distributor at VDE node 106 similar in nature to the one described above between VDE nodes 106 and 102) using the distribute process 1472B within the distributor's copy of the BUDGET method 1510B, a distribution and request/response/reply process similar to the one described above might be initiated. '193 patent at 172:61-174:29. **25(E)** Transportability of VDE Installations Between PPEs 650 In a preferred embodiment, VDE objects 300 and other secure information may, if appropriate, be transported from one PPE 650 to another securely using the various keys outlined above. VDE 100 uses redistribution of VDE administrative information to exchange ownership of VDE object 300, and to allow the portability of objects between electronic appliances 600. The permissions record 808 of VDE objects 300 contains rights information that may be used to determine whether an object can be redistributed in whole, in part, or at all. If a VDE object 300 can be redistributed, then electronic appliance 600 normally must have a "budget" and/or other permissioning that allows it to redistribute the object. For example, an electronic appliance 600 authorized to redistribute an object may create an administrative object containing a budget or rights less than or equal to the budget or rights that it owns. Some administrative objects may be sent to other PPEs 650. A PPE 650 that receives one of the administrative objects may have the ability to use at least a portion of the budgets, or rights, to related objects. '193 patent at 220:20-40.

	Claim Term / Phrase	InterTrust Evidence
		25(F) In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). '193 patent at 48:29-35. **25(G)** . . . plural, different control models regulating the use and/or auditing of either the same specific copy of electronic information content and/or differently regulating different copies (occurrences) of the same electronic information content. Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments. This includes supporting variable control information for budgeting and auditing usage as applied to a variety of predefined increments of electronic information, including employing a variety of different budgets and/or metering increments for a given electronic information deliverable for: billing units of measure, credit limit, security budget limit and security content metering increments, and/or market surveying and customer profiling content metering increments. '193 patent at 28:19-37. **25(H)** . . . support the flowing of content control information through different "branches" of content control information handling so as to accommodate, under the present invention's preferred embodiment, diverse controlled distributions of VDE controlled content. This allows different parties to employ the same initial electronic content with differing (perhaps competitive) control strategies. In this instance, a party who first placed control information on content can make certain control assumptions and these assumptions would evolve into more specific and/or extensive control assumptions. These control assumptions can evolve during the branching

	Claim Term / Phrase	InterTrust Evidence
		sequence upon content model participants submitting control information changes, for example, for use in "negotiating" with "in place" content control information. This can result in new or modified content control information and/or it might involve the selection of certain one or more already "in-place" content usage control methods over in-place alternative methods, as well as the submission of relevant control information parameter data. This form of evolution of different control information sets applied to different copies of the same electronic property content and/or appliance results from VDE control information flowing "down" through different branches in an overall pathway of handling and control and being modified differently as it diverges down these different pathway branches. '193 patent at 31:29-56. **25(I)** . . . multiple simultaneous control models for the same content property and/or property portion. This allows, for example, for concurrent business activities which are dependent on electronic commercial product content distribution, such as acquiring detailed market survey information and/or supporting advertising, both of which can increase revenue and result in lower content costs to users and greater value to content providers. Such control information and/or overall control models may be applied, as determined or allowed by control information, in differing manners to different participants in a pathway of content, reporting, payment, and/or related control information handling. VDE supports applying different content control information to the same and/or different content and/or appliance usage related activities, and/or to different parties in a content and/or appliance usage model, such that different parties (or classes of VDE users, for example) are subject to differing control information managing their use of electronic information content. For example, differing control models based on the category of a user as a distributor of a VDE controlled content object or an end-user of such content may result in different budgets being applied. Alternatively, for example, a one distributor may have the right to distribute a different array of properties than another distributor (from a common content collection provided, for example, on optical disc). An individual, and/or a class or other grouping of end-users, may have different costs (for example, a student, senior citizen, and/or poor citizen user of content who may

	Claim Term / Phrase	InterTrust Evidence
		be provided with the same or differing discounts) than a "typical" content user. '193 patent at 30:42-31:7. --- **25(J)** Such different application of control information may also result from content control information specifying that a certain party or group of parties shall be subject to content control information that differs from another party or group of parties. For example, content control information for a given piece of content may be stipulated as senior information and therefore not changeable, might be put in place by a content creator and might stipulate that national distributors of a given piece of their content may be permitted to make 100,000 copies per calendar quarter, so long as such copies are provided to bona fide end-users, but may pass only a single copy of such content to a local retailers and the control information limits such a retailer to making no more than 1,000 copies per month for retail sales to end-users. In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). '193 patent at 48:15-35. --- **25(K)** In this example, as illustrated in Figure 80, user B may receive control information associated with creator A's content from distributor A and/or user/distributor B. In either case, user B may be able to establish their own control information on DA(CA) and/or UDB(UDA(DA(CA))), respectively (if allowed by such control information. The resulting set(s) of control information UB(DA(CA)) and/or UB(UDB(UDA(DA(CA)))) respectively, may represent different control scenarios, each of which may have benefits for user B. As described in connection with an earlier example, user B may have received control information from user/distributor B along a chain of handling including user/distributor A that bases fees on the number of minutes that user B makes use of creator A's content (and requiring user/distributor A

	Claim Term / Phrase	InterTrust Evidence
		to pay fees of $15 per month per user to distributor A regardless of the amount of usage by user B in a calendar month). This may be more favorable under some circumstances than the fees required by a direct use of control information provided by distributor A, but may also have the disadvantage of an exhausted chain of redistribution and, for example, further usage information reporting requirements included in UDB(UDA(DA(CA))). If the two sets of control information DA(CA) and UDB(UDA(DA(CA))) permit (e.g. do not require exclusivity enforced, for example, by using a registration interval in an object registry used by a secure subsystem of user B's VDE installation to prevent deregistration and reregistration of different sets of control information related to a certain container (or registration of plural copies of the same content having different control information and/or being supplied by different content providers) within a particular interval of time as an aspect of an extended agreement for a chain of handling and control reflected in DA(CA) and/or UDB(UDA(DA(CA)))), user B may have both sets of control information registered and may make use of the set that they find preferable under a given usage scenario. '193 patent at 306:30-65. **25(L)** For example, user/distributor A may receive control information CB that includes a requirement that user/distributor A pay creator B for content decrypted by user/distributor A (and any participant receiving distributed and/or redistributed control information from user/distributor A) at the rate of $0.50 per kilobyte. As indicated above, user/distributor A also may receive control information associated with creator B's VDE content container from distributor A. In this example, user/distributor A may have a choice between paying a "rental" fee through a chain of handling passing through distributor A, and a fee based on the quantity of decryption through a chain of handling direct to creator B. In this case, user/distributor A may have the ability to choose to use either or both of CB and DA(CB). '193 patent at 308:29-42. **25(M)** As illustrated in Figure 81, in this example, user B may receive

	Claim Term / Phrase	InterTrust Evidence
		control information associated with creator B's VDE content container from six different sources: CB directly from creator B, DA(CB) from distributor A, UDB(UDA(DA(CB))) and/or UDB(UDA(CB)) from user/distributor B, DC(CB) from distributor C, and/or DB(DC(CB)) from distributor B. This represents six chains of handling through which user B may enter into extended agreements with other participants in this example. Two of these chains pass through user/distributor B. Based on a VDE negotiation between user/distributor B and user B, an extended agreement may be reached (if permitted by control information governing both parties) that reflects the conditions under which user B may use one or both sets of control information. In this example, two chains of handling and control may "converge" at user/distributor B, and then pass to user B (and if control information permits, later diverge once again based on distribution and/or redistribution by user B). '193 patent at 308:48-65. **25(N)** User B may, in this example, receive a VDE content container from distributor C that is comprised of VDE objects created by creator B, creator C, and creator D. In addition, user B may receive a VDE content container from distributor B that contains the same content created by creator B, creator C, and creator D in addition to one or more extracted/embedded portions of content created by creator E. User B may base decisions concerning which of such containers they choose to use (including which embedded containers she may wish to use), and under which circumstances, based on, for example, the character of such extracted/embedded portions (e.g. multimedia presentations illustrating potential areas of interest in the remainder of the content, commentary explaining and/or expositing other elements of content, related works, improved application software delivered as an element of content, etc.); the quality, utility, and/or price (or other attributes of control information) of such portions; and other considerations which distinguish the containers and/or content control information received, in this example, from distributor B and distributor C. '193 patent at 312:11-31.

	Claim Term / Phrase	InterTrust Evidence
		25(O) As with standard VDE objects 300, a user may be required to contact a clearinghouse service to acquire additional budgets if the user wishes to continue to use the traveling object after the exhaustion of an available budget(s) . . . . '193 patent at 131:10-13. --- **25(P)** Once the distributor 106 has used some or all of her budget, she may desire to obtain additional budget. The distributor 106 might then initiate a process using the BUDGET method request process (1480B). Request process 1480B might initiate a communication (1482AB) with the content creator VDE node 102 requesting more budget and perhaps providing details of the use activity to date (e.g., audit trails). The content creator 102 processes the 'get more budget' request event 1482AB using the response process (1484A) within the creator's BUDGET method 1510A. Response process 1484A might, for example, make a determination if the use information indicates proper use of the content, and/or if the distributor is credit worthy for more budget. The BUDGET method response process 1484A might also initiate a financial transaction to transfer funds from the distributor to pay for said use, or use the distribute process 1472A to distribute budget to the distributor 106. A response to the distributor 106 granting more budget (or denying more budget) might be sent immediately as a response to the request communication 1482AB, or it might be sent at a later time as part of a separate communication. The response communication, upon being received at the distributor's VDE node 106, might be processed using the reply process 1475B within the distributor's copy of the BUDGET method 1510B. The reply process 1475B might then process the additional budget in the same manner as described above. '193 patent at 173:21-174:14. --- **25(Q)** During the same or different communications exchange, the same or different clearinghouse may handle the end user's request for additional budget and/or permission pertaining to VDE object 300.

	Claim Term / Phrase	InterTrust Evidence
		For example, the end user's electronic appliance 600 may (e.g., in response to a user input request to access a particular VDE object 300) send an administrative object to the clearinghouse requesting budgets and/or other permissions allowing access (Block 1164). As mentioned above, such requests may be transmitted in the form of one or more administrative objects, such as, for example, a single administrative object having multiple "events" associated with multiple requested budgets and/or other permissions for the same or different VDE objects 300. The clearinghouse may upon receipt of such a request, check the end user's credit, financial records, business agreements and/or audit histories to determine whether the requested budgets and/or permissions should be given. The clearinghouse may, based on this analysis, send one or more responsive administrative objects which cause the end user's electronic appliance 600 to update its secure database in response (Block 1166, 1168). This updating might, for example, comprise replacing an expired PERC 808 with a fresh one, modifying a PERC to provide additional (or lesser) rights, etc. Steps 1164-1168 may be repeated multiple times in the same or different communications session to provide further updates to the end user's secure database 610. '193 patent at 162:39-65.

	Claim Term / Phrase	InterTrust Evidence
26.	193.1: "controlling the copies made of said digital file"	**Patent Specifications** **26(A)** . . . plural, different control models regulating the use and/or auditing of either the same specific copy of electronic information content and/or differently regulating different copies (occurrences) of the same electronic information content. Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments. This includes supporting variable control information for budgeting and auditing usage as applied to a variety of predefined increments of electronic information, including employing a variety of different budgets and/or metering increments for a given electronic information deliverable for: billing units of measure, credit limit, security budget limit and security content metering increments, and/or market surveying and customer profiling content metering increments. '193 patent at 28:19-37. **26(B)** . . . support the flowing of content control information through different "branches" of content control information handling so as to accommodate, under the present invention's preferred embodiment, diverse controlled distributions of VDE controlled content. This allows different parties to employ the same initial electronic content with differing (perhaps competitive) control strategies. In this instance, a party who first placed control information on content can make certain control assumptions and these assumptions would evolve into more specific and/or extensive control assumptions. These control assumptions can evolve during the branching sequence upon content model participants submitting control information changes, for example, for use in "negotiating" with "in place" content control information. This can result in new or modified content control information and/or it might involve the selection of certain one or more already "in-place" content usage control methods over in-place alternative methods, as well as the submission of relevant control information parameter data. This form of evolution of different control information sets applied to different copies of the same electronic property content and/or

	Claim Term / Phrase	InterTrust Evidence
		appliance results from VDE control information flowing "down" through different branches in an overall pathway of handling and control and being modified differently as it diverges down these different pathway branches. '193 patent at 31:29-56.
		26(C) . . . multiple simultaneous control models for the same content property and/or property portion. This allows, for example, for concurrent business activities which are dependent on electronic commercial product content distribution, such as acquiring detailed market survey information and/or supporting advertising, both of which can increase revenue and result in lower content costs to users and greater value to content providers. Such control information and/or overall control models may be applied, as determined or allowed by control information, in differing manners to different participants in a pathway of content, reporting, payment, and/or related control information handling. VDE supports applying different content control information to the same and/or different content and/or appliance usage related activities, and/or to different parties in a content and/or appliance usage model, such that different parties (or classes of VDE users, for example) are subject to differing control information managing their use of electronic information content. For example, differing control models based on the category of a user as a distributor of a VDE controlled content object or an end-user of such content may result in different budgets being applied. Alternatively, for example, a one distributor may have the right to distribute a different array of properties than another distributor (from a common content collection provided, for example, on optical disc). An individual and/or a class or other grouping of end-users, may have different costs (for example, a student, senior citizen, and/or poor citizen user of content who may be provided with the same or differing discounts) than a "typical" content user. '193 patent at 30:42-31:7.
		26(D) Such different application of control information may also result from content control information specifying that a certain party or

	Claim Term / Phrase	InterTrust Evidence
		group of parties shall be subject to content control information that differs from another party or group of parties. For example, content control information for a given piece of content may be stipulated as senior information and therefore not changeable, might be put in place by a content creator and might stipulate that national distributors of a given piece of their content may be permitted to make 100,000 copies per calendar quarter, so long as such copies are provided to bona fide end-users, but may pass only a single copy of such content to a local retailers and the control information limits such a retailer to making no more than 1,000 copies per month for retail sales to end-users. In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). '193 patent at 48:15-35. **26(E)** In this example, as illustrated in Figure 80, user B may receive control information associated with creator A's content from distributor A and/or user/distributor B. In either case, user B may be able to establish their own control information on DA(CA) and/or UDB(UDA(DA(CA))), respectively (if allowed by such control information. The resulting set(s) of control information UB(DA(CA)) and/or UB(UDB(UDA(DA(CA)))) respectively may represent different control scenarios, each of which may have benefits for user B. As described in connection with an earlier example, user B may have received control information from user/distributor B along a chain of handling including user/distributor A that bases fees on the number of minutes that user B makes use of creator A's content (and requiring user/distributor A to pay fees of $15 per month per user to distributor A regardless of the amount of usage by user B in a calendar month). This may be more favorable under some circumstances than the fees required by a direct use of control information provided by distributor A, but may also have the disadvantage of an exhausted chain of redistribution and, for example, further usage information reporting requirements included in UDB(UDA(DA(CA))). If the two sets of control information DA(CA) and UDB(UDA(DA(CA))) permit (e.g. do not require exclusivity enforced, for example, by using a registration interval in an object registry used by a secure subsystem of user B's VDE installation to prevent deregistration and

	Claim Term / Phrase	InterTrust Evidence
		built to execute only in SPE 503 secure space for government classes of security, or in an HPE 655 for commercial applications. As described above, the load module public header 802 may contain an "execution space code" field that indicates where the load module 1100 needs to execute. '193 patent at 140:15-46.

	Claim Term / Phrase	InterTrust Evidence
		reregistration of different sets of control information related to a certain container (or registration of plural copies of the same content having different control information and/or being supplied by different content providers) within a particular interval of time as an aspect of an extended agreement for a chain of handling and control reflected in DA(CA) and/or UDB(UDA(DA(CA)))), user B may have both sets of control information registered and may make use of the set that they find preferable under a given usage scenario. '193 patent at 306:30-65. **26(F)** For example, user/distributor A may receive control information CB that includes a requirement that user/distributor A pay creator B for content decrypted by user/distributor A (and any participant receiving distributed and/or redistributed control information from user/distributor A) at the rate of $0.50 per kilobyte. As indicated above, user/distributor A also may receive control information associated with creator B's VDE content container from distributor A. In this example, user/distributor A may have a choice between paying a "rental" fee through a chain of handling passing through distributor A, and a fee based on the quantity of decryption through a chain of handling direct to creator B. In this case, user/distributor A may have the ability to choose to use either or both of CB and DA(CB). '193 patent at 308:29-42. **26(G)** As illustrated in Figure 81, in this example, user B may receive control information associated with creator B's VDE content container from six different sources: CB directly from creator B, DA(CB) from distributor A, UDB(UDA(DA(CB))) and/or UDB(UDA(CB)) from user/distributor B, DC(CB) from distributor C, and/or DB(DC(CB)) from distributor B. This represents six chains of handling through which user B may enter into extended agreements with other participants in this example. Two of these chains pass through user/distributor B. Based on a VDE negotiation between user/distributor B and user B, an extended agreement may be reached (if permitted by control information governing both parties) that reflects the conditions under which user B may use one

	Claim Term / Phrase	InterTrust Evidence
		or both sets of control information. In this example, two chains of handling and control may "converge" at user/distributor B, and then pass to user B (and if control information permits, later diverge once again based on distribution and/or redistribution by user B). '193 patent at 308:48-65. **26(H)** User B may, in this example, receive a VDE content container from distributor C that is comprised of VDE objects created by creator B, creator C, and creator D. In addition, user B may receive a VDE content container from distributor B that contains the same content created by creator B, creator C, and creator D in addition to one or more extracted/embedded portions of content created by creator E. User B may base decisions concerning which of such containers they choose to use (including which embedded containers she may wish to use), and under which circumstances, based on, for example, the character of such extracted/embedded portions (e.g. multimedia presentations illustrating potential areas of interest in the remainder of the content, commentary explaining and/or expositing other elements of content, related works, improved application software delivered as an element of content, etc.); the quality, utility, and/or price (or other attributes of control information) of such portions; and other considerations which distinguish the containers and/or content control information received, in this example, from distributor B and distributor C. '193 patent at 312:11-31.

	Claim Term / Phrase	InterTrust Evidence
27.	721.1: "digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class"	**Patent Specifications** **27(A)** In accordance with one aspect provided by the present invention, one or more trusted verifying authorities validate load modules or other executables by analyzing and/or testing them. A verifying authority digitally "signs" and "certifies" those load modules or other executables it has verified (using a public key based digital signature and/or certificate based thereon, for example). Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. '721 patent at 4:61-5:5. --- **27(B)** A hierarchy of assurance levels may be provided for different protected processing environment security levels. Load modules or other executables can be provided with digital signatures associated with particular assurance levels. Appliances assigned to particular assurance levels can protect themselves from executing load modules or other executables associated with different assurance levels. Different digital signatures and/or certificates may be used to distinguish between load modules or other executables intended for different assurance levels. This strict assurance level hierarchy provides a framework to help ensure that a more trusted environment can protect itself from load modules or other executables exposed to environments with different work factors (e.g., less trusted or tamper resistant environments). This can be used to provide a high degree of security compartmentalization that helps protect the remainder of the system should parts of the system become compromised. For example, protected processing environments or other secure execution spaces that are more impervious to tampering (such as those providing a higher degree of physical security) may use an assurance level that isolates it from protected processing environments or other secure execution spaces that are relatively more susceptible to tampering (such as those constructed solely by software executing on a general purpose digital computer in a non-

	Claim Term / Phrase	InterTrust Evidence
		secure location). A verifying authority may digitally sign load modules or other executables with a digital signature that indicates or implies assurance level. A verifying authority can use digital signature techniques to distinguish between assurance levels. As one example, each different digital signature may be encrypted using a different verification key and/or fundamentally different encryption, one-way hash and/or other techniques. A protected processing environment or other secure execution space protects itself by executing only those load modules or other executables that have been digitally signed for its corresponding assurance level. The present invention may use a verifying authority and the digital signatures it provides to compartmentalize the different electronic appliances depending on their level of security (e.g., work factor or relative tamper resistance). In particular, a verifying authority and the digital signatures it provides isolate appliances with significantly different work factors — preventing the security of high work factor appliances from collapsing into the security of low work factor appliances due to free exchange of load modules or other executables. '721 patent at 6:16-62. **27(C)** Figures 11A-11C show how a verifying authority can use different digital signatures to designate the same or different load modules as being appropriate for execution by different assurance level electronic appliances; Figures 12, 13 and 13A show how assurance level digital signatures can be used to isolate electronic appliances or appliance types based on work factor and/or tamper resistance to reduce overall security risks; '721 patent at 7:66-8:6.

	Claim Term / Phrase	InterTrust Evidence
		27(D) Assurance Levels Verifying authority 100 can use different digital signing techniques to provide different "assurance levels" for different kinds of electronic appliances 61 having different "work factors" or levels of tamper resistance. Figures 10A-10C show an example assurance level hierarchy providing three different assurance levels for different electronic appliance types: Assurance level I might be used for an electronic appliance(s) 61 whose protected processing environment 108 is based on software techniques that may be somewhat resistant to tampering. An example of an assurance level I electronic appliance 61A might be a general purpose personal computer that executes software to create protected processing environment 108. An assurance level II electronic appliance 61B may provide a protected processing environment 108 based on a hybrid of software security techniques and hardware-based security techniques. An example of an assurance level II electronic appliance 61B might be a general purpose personal computer equipped with a hardware integrated circuit secure processing unit ("SPU") that performs some secure processing outside of the SPU (see Ginter et al. patent disclosure Figure 10 and associated text). Such a hybrid arrangement might be relatively more resistant to tampering than a software-only implementation. The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. Figures 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance. In this example, verifying authority 100 digitally signs load modules 54 using different digital signature techniques (for example, different "private" keys 122) based on assurance level. The digital signatures 106 applied by verifying authority 100 thus securely encode the same (or different) load module 54 for use by appropriate corresponding assurance level electronic appliances 61. Assurance level in this example may be assigned to a particular

	Claim Term / Phrase	InterTrust Evidence
		protected processing environment 108 at initialization (e.g., at the factory in the case of hardware-based secure processing units). Assigning assurance level at initialization time facilitates the use of key management (e.g., secure key exchange protocols) to enforce isolation based on assurance level. For example, since establishment of assurance level is done at initialization time, rather than in the field in this example, the key exchange mechanism can be used to provide new keys (assuming an assurance level has been established correctly). '721 patent at 16:37-17:23. **27(E)** In one example, verifying authority 100 may digitally sign identical copies of load module 54 for use by different classes or "assurance levels" of electronic appliances 61. If the sharing of a load module 54 between different electronic appliances is regarded as an open communications channel between the protected processing environments 108 of the two appliances, it becomes apparent that there is a high degree of risk in permitting such sharing to occur. In particular, the extra security assurances and precautions of the more trusted environment are collapsed into the those of the less trusted environment because an attacker who compromises a load module within a less trusted environment is then be able to launch the same load module to attack the more trusted environment. Hence, although compartmentalization based on encryption and key management can be used to restrict certain kinds of load modules 54 to execute only on certain types of electronic appliances 61, a significant application in this context is to compartmentalize the different types of electronic appliances and thereby allow an electronic appliance to protect itself against load modules 54 of different assurance levels. '721 patent at 18:19-38. **27(F)** In accordance with this feature of the invention, verifying authority 100 supports all of these various categories of digital signatures, and system 50 uses key management to distribute the appropriate verification keys to different assurance level devices. For example, verifying authority 100 may digitally sign a particular load module

	Claim Term / Phrase	InterTrust Evidence
		54 such that only hardware-only based server(s) 402(3) at assurance level XI may authenticate it. This compartmentalization prevents any load module executable on hardware-only servers 402(3) from executing on any other assurance level appliance (for example, software-only protected processing environment based support service 404(1)). To simplify key management and distribution, execution environments having significantly similar work factors can be classified in the same assurance level. Figure 13 shows one example hierarchical assurance level arrangement. In this example, less secure "software only" protected processing environment 108 devices are categorized as assurance level I, somewhat more secure "software and hardware hybrid" protected processing environment appliances are categorized as assurance level II, and more trusted "hardware only" protected processing environment devices are categorized as assurance level III. '721 patent at 19:11-32. --- **27(G)** A load module or other executable may be certified for multiple assurance levels. Different digital signatures may be used to certify the same load module or other executable for different respective assurance levels. '721 patent at 20:1-4.

	Claim Term / Phrase	InterTrust Evidence
28.	891.1: "securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item"	**Patent Specifications** **28(A)** The embedding processes for all VDE embedded content containers normally involves securely identifying the appropriate content control information for the embedded content. For example, VDE content control information for a VDE installation and/or a VDE content container may securely, and transparently to an embedder (user), apply the same content control information to edited (such as modified or additional) container content as is applied to one or more portions (including all, for example) of previously "in place" content of said container and/or securely apply control information generated through a VDE control information negotiation between control sets, and/or it may apply control information previously applied to said content. Application of control information may occur regardless of whether the edited content is in a parent or embedded container. This same capability of securely applying content control information (which may be automatically and/or transparently applied), may also be employed with content that is embedded into a VDE container through extracting and embedding content, or through the moving, or copying and embedding, of VDE container objects. Application of content control information normally occurs securely within one or more VDE secure sub-system PPEs 650. This process may employ a VDE template that enables a user, through easy to use GUI user interface tools, to specify VDE content control information for certain or all embedded content, and which may include menu driven, user selectable and/or definable options, such as picking amongst alternative control methods (e.g. between different forms of metering) which may be represented by different icons picturing (symbolizing) different control functions and apply such functions to an increment of VDE secured content, such as an embedded object listed on an object directory display. '193 patent at 299:19-51. --- **28(B)** Embedded content (and/or content objects) may have been contributed by different parties and may be integrated into a VDE container through a VDE content and content control information integration process securely managed through the use of one or more secure VDE subsystems. This process may, for example, involve one or more of:

	Claim Term / Phrase	InterTrust Evidence
		(1.) securely applying instructions controlling the embedding and/or use of said submitted content, wherein said instructions were securely put in place, at least in part, by a content provider and/or user of said VDE container. For example, said user and/or provider may interact with one or more user interfaces offering a selection of content embedding and/or control options (e.g. in the form of a VDE template). Such options may include which, and/or whether, one or more controls should be applied to one or more portions of said content and/or the entry of content control parameter data (such a time period before which said content may not be used, cost of use of content, and/or pricing discount control parameters such as software program suite sale discounting). Once required and/or optional content control information is established by a provider and/or user, it may function as content control information which may be, in part or in full, applied automatically to certain, or all, content which is embedded in a VDE content container. '193 patent at 300:6-30. **28(C)** Users of VDE may include content creators who apply content usage, usage reporting, and/or usage payment related control information to electronic content and/or appliances for users such as end-user organizations, individuals, and content and/or appliance distributors. '193 patent at 9:40-45. **28(D)** For example, in a VDE aware word processor application, a user may be able to "print" a document into a VDE content container object, applying specific control information by selecting from amongst a series of different menu templates for different purposes (for example, a confidential memo template for internal organization purposes may restrict the ability to "keep," that is to make an electronic copy of the memo). '193 patent at 26:59-67.

	Claim Term / Phrase	InterTrust Evidence
		28(E) VDE supports applying different content control information to the same and/or different content and/or appliance usage related activities, and/or to different parties in a content and/or appliance usage model, such that different parties (or classes of VDE users, for example) are subject to differing control information managing their use of electronic information content. For example, differing control models based on the category of a user as a distributor of a VDE controlled content object or an end-user of such content may result in different budgets being applied. '193 patent at 30:55-65. **28(F)** Keys and tags may be securely generated within SPE 503 (HPE 655) in the preferred embodiment. '193 patent at 120:15-16. **28(G)** Frequently, for a VDE application for a given content model (such as distribution of entertainment on CD-ROM, content delivery from an Internet repository, or electronic catalog shopping and advertising, or some combination of the above) participants would be able to securely select from amongst available, alternative control methods and apply related parameter data, wherein such selection of control method and/or submission of data would constitute their "contribution" of control information. '193 patent at 18:60-19:1. **28(H)** ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655). '193 patent at 83:44-48

	Claim Term / Phrase	InterTrust Evidence
29.	900.155: "derives information from one or more aspects of said host processing environment"	**Patent Specifications** **29(A)** Correspondence Between Installed Software and Appliance "Signature". Another technique that may be used during the installation routine 3470 is to customize the operational materials 3472 by embedding a "machine signature" into the operational materials to establish a correspondence between the installed software on a particular electronic appliance 600 (Figure 69C, block 3470(7)). This technique prevents a software-based PPE 650 from being transferred from one electronic appliance 600 to another (except through the use of the appropriate secure, verified backup mechanism). For electronic appliances 600 where it is feasible to do so, the installation procedure 3470 may determine unique information about the electronic appliance 600 (e.g., a "signature" SIG in the sense of a unique value - not necessarily a "digital signature" in the cryptographic sense). Installation routine 3470 embeds the electronic appliance "signature" SIG in the installed operational materials 3472. Upon initialization, the operational materials 3472 validate the embedded signature value against the actual electronic appliance 600 signature SIG, and may refuse to start if the comparison fails. Depending on the configuration of electronic appliance 600, the machine signature may consist, for example, of some combination of a hash of the ROM BIOS 658 (see Figure 69G); a hash of a disk defect map 3497a; the Ethernet (or other) network adapter 666 address; information written into an unused disk sector; information stored in a non-volatile CMOS RAM (such as used for hardware configuration data); information stored in non-volatile ("flash") memory (such as used for system or peripheral component "BIOS" programs) and/or hidden unique information placed into the root directory 3497b of the fixed disk drive 668.

	Claim Term / Phrase	InterTrust Evidence
		Figure 69G shows an example of some of these appliance-specific signatures. '900 patent at 239:4-42.

	Claim Term / Phrase	InterTrust Evidence
30.	912.8: "identifying at least one aspect of an execution space required for use and/or execution of the load module"	**Patent Specifications** **30(A)** The following is an example of a possible field layout for load module public header 802:

Field Type		Description
LM ID		VDE ID of Load Module.
	Creator ID	Site ID of creator of this load module.
	Type ID	Constant indicates load module type.
	LM ID	Unique sequence number for this load module, which uniquely identifies the load module in a sequence of load modules created by an authorized VDE participant.
	Version ID	Version number of this load module.
Other classification information	Class ID	ID to support different load module classes.
	Type ID	ID to support method type compatible searching.
Descriptive Information	Description	Textual description of the load module.
	Execution space code	Value that describes what execution space (e.g., SPE or HPE) this load module

Many load modules 1100 contain code that executes in an SPE 503. Some load modules 1100 contain code that executes in an HPE 655. This allows methods 1000 to execute in whichever environment is appropriate. For example, an INFORMATION method 1000 can be built to execute only in SPE 503 secure space for government classes of security, or in an HPE 655 for commercial applications. As described above, the load module public header 802 may contain an "execution space code" field that indicates where the load module 1100 needs to execute.

'193 patent at 140:15-46.